

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002359623 A

(43) Date of publication of application: 13.12.02

(51) Int. Cl **H04L 12/28**
H04L 29/06
H04Q 7/22
H04Q 7/24
H04Q 7/26
H04Q 7/30
H04Q 7/38

(21) Application number: 2002045145

(22) Date of filing: 21.02.02

(30) Priority: 27.03.01 JP 2001091423

(71) Applicant: SEIKO EPSON CORP

(72) Inventor: MIYAKOSHI DAISUKE
MUTO KAZUHIKO
YAMAKADO HITOSHI
MIYAMOTO TORU

**(54) WIRELESS COMMUNICATION SETTING
METHOD, COMMUNICATION TERMINAL,
ACCESS POINT TERMINAL, RECORDING
MEDIUM AND PROGRAM**

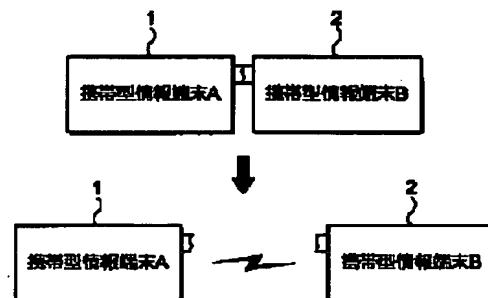
two wireless communication terminals.

COPYRIGHT: (C)2003,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To simply make settings of wireless communication parameters.

SOLUTION: First, by connecting a wireless communication terminal, which has a cable communication unit, to another wireless communication terminal, which also has a cable communication unit, via their respective cable communication units, guide information, which is required to determine communication parameters for wireless communication between the two wireless communication terminals using their respective wireless communication units, is communicated under the connection. Next, the communication parameters are determined on the basis of the guide information, and determined communication parameters are communicated under the connection. Next, the communication parameters are applied to the two wireless communication terminals automatically. Consequently, users of the two wireless communication terminals can start a wireless communication between the



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-359623
(P2002-359623A)

(43)公開日 平成14年12月13日 (2002.12.13)

(51)Int.Cl. ¹	識別記号	F I	テ-マコ-ト [®] (参考)
H 04 L 12/28	3 0 0	H 04 L 12/28	3 0 0 Z 5 K 0 3 3
29/06			3 0 0 A 5 K 0 3 4
H 04 Q 7/22		13/00	3 0 5 C 5 K 0 6 7
7/24		H 04 Q 7/04	A
		H 04 B 7/26	1 0 9 M
			審査請求 未請求 請求項の数22 O L (全 41 頁) 最終頁に続く

(21)出願番号 特願2002-45145(P2002-45145)

(22)出願日 平成14年2月21日 (2002.2.21)

(31)優先権主張番号 特願2001-91423(P2001-91423)

(32)優先日 平成13年3月27日 (2001.3.27)

(33)優先権主張国 日本 (JP)

(71)出願人 000002369

セイコーエプソン株式会社
東京都新宿区西新宿2丁目4番1号(72)発明者 宮腰 大輔
長野県諏訪市大和3丁目3番5号 セイコ
一エプソン株式会社内(72)発明者 無藤 和彦
長野県諏訪市大和3丁目3番5号 セイコ
一エプソン株式会社内(74)代理人 100098084
弁理士 川▲崎▼ 研二

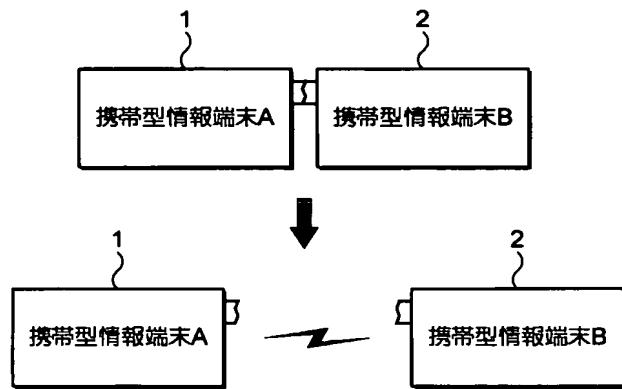
最終頁に続く

(54)【発明の名称】 無線通信設定方法、通信端末、アクセスポイント端末、記録媒体およびプログラム

(57)【要約】

【課題】 無線通信におけるパラメータ設定を簡易に行う。

【解決手段】 無線通信端末が有する有線通信部と他の無線通信端末が有する有線通信部を接続することにより、まず、前記無線通信端末が前記他の無線通信端末と無線通信を行うにあたり必要となる通信パラメータを決定するための案内情報が、前記接続において送受信される。続いて、その案内情報に基づいて前記通信パラメータが決定され、決定された通信パラメータが前記接続において送受信される。さらに、前記通信パラメータが前記無線通信端末および前記他の無線通信端末に自動的に設定される。その結果、前記無線通信端末のユーザは簡単に前記無線通信端末と前記他の無線通信端末との無線通信を開始できる。



【特許請求の範囲】

【請求項1】 無線通信が可能な第1通信部と前記第1通信部とは異なる第2通信部とを有する第1通信機器と第2通信機器が、それぞれの前記第2通信部を互いに接続する接続段階と、

前記第1通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記案内情報を、前記第2通信部を用いて受信する案内情報通信段階と、

前記第2通信機器が、前記第1通信機器と前記第2通信機器が各々の前記第1通信部を利用して通信を行うための通信パラメータを、前記案内情報を用いて決定する通信パラメータ決定段階と、

を備えることを特徴とする通信パラメータ設定方法。

【請求項2】 請求項1における通信パラメータ設定方法であって、

前記通信パラメータ決定段階の後に、

前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを、前記第1通信部を利用した前記第1通信機器との通信に用いられる状態にする通信パラメータ設定段階を備えることを特徴とする通信パラメータ設定方法。

【請求項3】 請求項1における通信パラメータ設定方法であって、

前記通信パラメータ決定段階の後に、

前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記通信パラメータを前記第2通信部を用いて受信する通信パラメータ通信段階と、

前記第1通信機器が、前記通信パラメータを、前記第1通信部を利用した前記第2通信機器との通信に用いられる状態にする通信パラメータ設定段階を備えることを特徴とする通信パラメータ設定方法。

【請求項4】 請求項1における通信パラメータ設定方法であって、

前記通信パラメータ決定段階の後に、

前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記通信パラメータを前記第2通信部を用いて受信する通信パラメータ通信段階と、

前記第1通信機器と前記第2通信機器が、前記通信パラメータを、それぞれの前記第1通信部を利用した相互の通信に用いられる状態にする通信パラメータ設定段階を備えることを特徴とする通信パラメータ設定方法。

【請求項5】 請求項1における通信パラメータ設定方法であって、

前記接続段階における接続は、前記第1通信機器と前記

第2通信機器のそれぞれの前記第2通信部を直接接觸させることによる接続であることを特徴とする通信パラメータ設定方法。

【請求項6】 請求項1における通信パラメータ設定方法であって、

前記接続段階における接続は、第1通信機器と前記第2通信機器の前記第1通信部を利用する無線通信と比べて近距離の無線通信による接続であることを特徴とする通信パラメータ設定方法。

【請求項7】 請求項1における通信パラメータ設定方法であって、

前記第1通信機器および前記第2通信機器は共に通信端末であることを特徴とする通信パラメータ設定方法。

【請求項8】 請求項1における通信パラメータ設定方法であって、

前記第1通信機器または前記第2通信機器は他の通信機器が無線通信を行う際にその通信の中継を行うアクセスポイントであることを特徴とする通信パラメータ設定方法。

【請求項9】 請求項1における通信パラメータ設定方法であって、

前記通信パラメータ決定段階において、前記第2通信機器は前記第1通信部を利用する通信において用いる1つもしくは複数の通信プロトコルを選択する通信プロトコル選択段階を備えることを特徴とする通信パラメータ設定方法。

【請求項10】 請求項1における通信パラメータ設定方法であって、

前記通信パラメータは有線通信と無線通信に共通して用いられる通信プロトコルに関するパラメータを含むことを特徴とする通信パラメータ設定方法。

【請求項11】 請求項1における通信パラメータ設定方法であって、

前記第1通信機器が、前記第2通信機器が前記第1通信部を利用して送受信する情報を暗号化もしくは復号化するための暗号鍵情報を前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が、前記暗号鍵情報を前記第2通信部を用いて受信する暗号鍵情報通信段階を備え、

前記第2通信機器は前記暗号鍵情報によって、前記第1通信部を利用して送受信する情報を暗号化もしくは復号化することを特徴とする通信パラメータ設定方法。

【請求項12】 請求項1における通信パラメータ設定方法であって、

前記第2通信機器が、前記第1通信機器が前記第1通信部を利用して送受信する情報を暗号化もしくは復号化するための暗号鍵情報を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記暗号鍵情報を前記第2通信部を用いて受信する暗号鍵情報通信段階を備え、

前記第1通信機器は前記暗号鍵情報によって、前記第1通信部を利用して送受信する情報を暗号化もしくは復号化することを特徴とする通信パラメータ設定方法。

【請求項13】 請求項1における通信パラメータ設定方法であって、

前記第1通信機器が前記第1通信機器を特定する識別子を前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、

前記第2通信機器は前記識別子を用いて、前記第1通信機器が前記第1通信部を利用する前記第2通信機器との通信を行うことの許可または拒否を行うことを特徴とする通信パラメータ設定方法。

【請求項14】 請求項1における通信パラメータ設定方法であって、

前記第2通信機器が前記第2通信機器を特定する識別子を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、

前記第1通信機器は前記識別子を用いて、前記第2通信機器が前記第1通信部を利用する前記第1通信機器との通信を行うことの許可または拒否を行うことを特徴とする通信パラメータ設定方法。

【請求項15】 請求項1における通信パラメータ設定方法であって、

前記第1通信機器が前記第1通信機器を特定する識別子を前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、

前記第2通信機器は前記識別子に基づいて、前記第1通信機器が前記第1通信部を利用して行う通信におけるネットワーク資源の利用可能な範囲を決定することを特徴とする通信パラメータ設定方法。

【請求項16】 請求項1における通信パラメータ設定方法であって、

前記第2通信機器が前記第2通信機器を特定する識別子を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、

前記第1通信機器は前記識別子を用いて、前記第2通信機器が前記第1通信部を利用して行う通信におけるネットワーク資源の利用可能な範囲を決定することを特徴とする無線通信パラメータ設定方法。

【請求項17】 無線通信が可能な第1通信部と、

前記第1通信部とは異なる第2通信部と、

記憶部と、

前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を前記第2通信部を用いて他の通信機器に送信する制御部とを備えることを特徴とする通信機器。

【請求項18】 無線通信が可能な第1通信部と、前記第1通信部とは異なる第2通信部と、記憶部と、

この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて受信し、この通信機器と前記第2通信機器が前記第1通信部を利用して通信を行うための通信パラメータを前記案内情報を用いて決定する制御部とを備えることを特徴とする通信機器。

【請求項19】 無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、

前記第2通信部により他の通信機器との通信が可能になったことを検知させ、

前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を前記第2通信部を用いて前記他の通信機器に送信させるプログラムを記録してなるコンピュータ読み取り可能な記録媒体。

【請求項20】 無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、

前記第2通信部により他の通信機器との通信が可能になったことを検知させ、

この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて受信し、

この通信機器と前記第2通信機器が前記第1通信部を利用して通信を行うための通信パラメータを前記案内情報を用いて決定させるプログラムを記録してなるコンピュータ読み取り可能な記録媒体。

【請求項21】 無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、

前記第2通信部により他の通信機器との通信が可能になったことを検知させ、

前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を前記第2通信部を用いて前記他の通信機器に送信させるプログラム。

【請求項22】 無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、

前記第2通信部により他の通信機器との通信が可能になったことを検知させ、

この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて受信し、

この通信機器と前記第2通信機器が前記第1通信部を利

用して通信を行うための通信パラメータを前記案内情報用いて決定させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、特定区域内情報通信網（LAN）のためのパラメータ設定方法、通信端末、アクセスポイント、記録媒体およびプログラムに係り、特に、無線LANのための各種設定を行うための技術に関する。

【0002】

【従来の技術】通信網に新たに通信端末を接続するには、一般的に次のような手順を踏む。まず通信端末のユーザが、自分の通信端末が利用可能な通信プロトコルに関する情報を通信網の管理者に伝える。次に管理者が通信網において利用可能な通信プロトコルの情報と、通信端末のユーザから得た通信端末が利用可能な通信プロトコルの情報を考慮して、通信網と通信端末の両方が利用可能な通信プロトコルを1つもしくは複数選択する。続いて、管理者は選択した通信プロトコルのパラメータから変更を加える必要があるものを決定し、その決定したパラメータを通信端末のユーザに伝える。ユーザはこのパラメータを通信端末に設定する。上記のパラメータは通常、管理者以外は知らない情報を含んでいる。このため、例えば管理者が不在の場合には設定作業を行うことができない。また、たとえ必要なパラメータが得られたとしても、そのパラメータを用いて通信端末の設定を正しく迅速に行なうことは、通常のユーザにとって容易ではない。更に、専門的な技術知識を持つ管理者であっても、利用可能な通信プロトコルが複数存在する場合、それぞれの通信プロトコルの通信速度等を考慮して、それらの通信プロトコルから適する通信プロトコルを選択することは容易ではない。

【0003】以上の事情から、必要なパラメータの設定を自動化することに対するニーズは高い。そのニーズに対し、まず、有線通信と無線通信に共通する中位および高位のレイヤのプロトコルに関するパラメータ設定を自動化する技術的努力がなされている。その例として、DHCP (Dynamic Host Configuration Protocol) サーバの利用がある。インターネットの普及に伴い多くの人がTCP/IP (Transmission Control Protocol / Internet Protocol) を利用しているが、TCP/IPにおいてはIPアドレスを通信網上の全ての通信機器に重複することなく割り当てる必要がある。以前は管理者がこの作業を手動で行い、ユーザは管理者から割り当てられたIPアドレスを自分の通信端末に手動で設定する必要があった。現在、DHCPサーバ・プログラムのインストールされた通信機器が通信網内の通信機器にIPアドレスを自動的に割り当て、DHCPクライアント・プログラムのインストールされた通信機器が、その通信機器に割り当てられたIPアドレスを自動的に受信し、設定することが広く行われている。

【0004】更に、利用する通信網が無線通信網である場合に、無線通信用の低位レイヤのプロトコルに関するパラメータ設定に関しては、有線通信と無線通信に共通する中位および高位のレイヤのプロトコルに関するパラメータ設定以上に、その自動化に対するニーズが高い。その主たる理由は、通信プロトコルの数が多いことによる。低位レイヤのプロトコルに関して、有線通信網においては現在IEEE802.3(Ethernet、Fast Ethernet)がほぼ標準として定着しているのに対し、無線通信網においてはIEEE802.11bやBluetoothのように定着しつつある通信プロトコルが複数存在する。さらに、IEEE802.11a、IEEE802.15、IEEE802.16等の新たな通信プロトコルも登場しつつある。加えて、これらの無線通信網用の通信プロトコルの一部は同じ周波数帯を利用することから、場合によってはある通信プロトコルを用いるために他の通信プロトコルの使用を制限する必要がある。従って、無線通信網における通信プロトコルの選択は有線通信網におけるものより複雑である。これに対し、無線通信用の低位レイヤのプロトコルに関するパラメータ設定自動化の技術として、周波数チャンネルの自動ネゴシエーションがある。これは、無線通信機器が一定の条件を満たす電波圏に入ると、無線通信機器がその電波の発信元の通信機器と相互に利用可能な周波数チャンネルを探し出し、その周波数チャンネルが無線通信機器に自動的に設定される、という技術である。

【0005】

【発明が解決しようとする課題】しかしながら、無線通信網に接続する際の設定は依然として手入力による部分が多い。その背景には、無線通信網においては有線通信網における場合と比較し、部外者が見えないところで接続を行い、通信情報の盗聴を行う可能性が高い、という事情がある。無線通信網においては、それらの通信情報の盗聴を防ぐため、有線通信網の場合と異なり、通常、低位レイヤのプロトコルにおいて接続認証およびデータの暗号化が行われる。これらの認証および暗号化のためのパラメータ設定は、セキュリティ上の理由から手入力によらざるを得ず、煩雑さが解消されていない。更に、上述の従来技術によっても、無線通信網において利用可能な通信プロトコルが複数存在する場合にそれら複数の通信プロトコルから最適なものを選択する際の困難さは解消されていない。

【0006】本発明は上述した事情に鑑みてなされたものであり、無線通信網において新たな通信端末を接続する際、誰もが簡易に望ましい通信プロトコルを選択し、その選択された通信プロトコルを利用するにあたり必要となるパラメータ設定を行うことを可能とする無線通信設定方法、通信端末、アクセスポイント、記録媒体およびプログラムを提供することを目的としている。

【0007】

【課題を解決するための手段】上述した課題を解決する

ために、本発明に係る通信パラメータ設定方法は、無線通信が可能な第1通信部と前記第1通信部とは異なる第2通信部とを有する第1通信機器と第2通信機器が、それぞれの前記第2通信部を互いに接続する接続段階と、前記第1通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記案内情報を、前記第2通信部を用いて受信する案内情報通信段階と、前記第2通信機器が、前記第1通信機器と前記第2通信機器が各々の前記第1通信部を利用して通信を行うための通信パラメータを、前記案内情報を用いて決定する通信パラメータ決定段階とを備えることを特徴としている。これを本発明の第1態様と呼ぶ。この通信パラメータ設定方法によると、第1通信機器と第2通信機器の各々の第2通信部を接続することにより、第2通信機器において、無線通信を行うための通信パラメータが決定される。これにより、ユーザは無線通信に必要な通信パラメータを自分で決定する必要がなくなる。

【0008】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記通信パラメータ決定段階の後に、前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを、前記第1通信部を利用した前記第1通信機器との通信に用いられる状態にする通信パラメータ設定段階を備えてもよい。この通信パラメータ設定方法によると、無線通信を行うにあたり第2通信機器の通信パラメータに変更を加える必要がある場合、ユーザはその変更を要する通信パラメータを自分で設定する必要がなくなる。

【0009】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記通信パラメータ決定段階の後に、前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記通信パラメータを前記第2通信部を用いて受信する通信パラメータ通信段階と、前記第1通信機器が、前記通信パラメータを、前記第1通信部を利用した前記第2通信機器との通信に用いられる状態にする通信パラメータ設定段階を備えてもよい。この通信パラメータ設定方法によると、無線通信を行うにあたり第1通信機器の通信パラメータに変更を加える必要がある場合、ユーザはその変更を要する通信パラメータを自分で設定する必要がなくなる。

【0010】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記通信パラメータ決定段階の後に、前記第2通信機器が、前記通信パラメータ決定段階において決定された通信パラメータを前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記通信パラメータを前記第2通信部を用いて受信する通信パラメータ通信段階と、前記第1通信

機器と前記第2通信機器が、前記通信パラメータを、それぞれの前記第1通信部を利用した相互の通信に用いられる状態にする通信パラメータ設定段階を備えてもよい。この通信パラメータ設定方法によると、無線通信を行うにあたり第1通信機器の通信パラメータおよび第2通信機器の通信パラメータに変更を加える必要がある場合、ユーザはその変更を要する通信パラメータを自分で設定する必要がなくなる。

【0011】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記接続段階における接続は、前記第1通信機器と前記第2通信機器のそれぞれの前記第2通信部を直接接触させることによる接続であってもよい。この通信パラメータ設定方法によると、ユーザは第1通信機器および第2通信機器に対し、より直感的に通信パラメータ設定の指示を行うことができる。

【0012】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記接続段階における接続は、第1通信機器と前記第2通信機器の前記第1通信部を利用する無線通信と比べて近距離の無線通信による接続であってもよい。この通信パラメータ設定方法によると、第1通信機器もしくは第2通信機器がケーブル等を用いた接続を行うにあたり困難な場所に位置している場合であっても、ユーザは容易に通信パラメータ設定の指示を行うことができる。

【0013】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第1通信機器および前記第2通信機器は共に通信端末であってもよい。

【0014】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第1通信機器または前記第2通信機器は他の通信機器が無線通信を行う際にその通信の中継を行うアクセスポイントであってもよい。

【0015】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記通信パラメータ決定段階において、前記第2通信機器は前記第1通信部を利用する通信において用いる1つもしくは複数の通信プロトコルを選択する通信プロトコル選択段階を備えてもよい。この通信パラメータ設定方法によると、ユーザは無線通信に用いる通信プロトコルを自分で選択する必要がなくなる。

【0016】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記通信パラメータは有線通信と無線通信に共通して用いられる通信プロトコルに関するパラメータを含んでもよい。

【0017】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第1通信機器が、前記第2通信機器が前記第1通信部を利用して送受信する情報を暗号化もしくは復号化するための暗号鍵情報を前記第2通信部を用いて前記第2通信機器に送信し、前

記第2通信機器が、前記暗号鍵情報を前記第2通信部を用いて受信する暗号鍵情報通信段階を備え、前記第2通信機器は前記暗号鍵情報によって、前記第1通信部を利用して送受信する情報を暗号化もしくは復号化してもよい。この通信パラメータ設定方法によると、第2通信機器のユーザは特別な設定を行うことなく、通信情報の漏洩を防止できる。

【0018】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第2通信機器が、前記第1通信機器が前記第1通信部を利用して送受信する情報を暗号化もしくは復号化するための暗号鍵情報を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が、前記暗号鍵情報を前記第2通信部を用いて受信する暗号鍵情報通信段階を備え、前記第1通信機器は前記暗号鍵情報によって、前記第1通信部を利用して送受信する情報を暗号化もしくは復号化してもよい。この通信パラメータ設定方法によると、第2通信機器のユーザは特別な設定を行うことなく、通信情報の漏洩を防止できる。

【0019】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第1通信機器が前記第1通信機器を特定する識別子を前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、前記第2通信機器は前記識別子を用いて、前記第1通信機器が前記第1通信部を利用する前記第2通信機器との通信を行うことの許可または拒否を行ってもよい。この通信パラメータ設定方法によると、第1通信機器が許可なく第2通信機器に接続されることが防止される。

【0020】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第2通信機器が前記第2通信機器を特定する識別子を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、前記第1通信機器は前記識別子を用いて、前記第2通信機器が前記第1通信部を利用する前記第1通信機器との通信を行うことの許可または拒否を行ってもよい。この通信パラメータ設定方法によると、第2通信機器が許可なく第1通信機器に接続されることが防止される。

【0021】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第1通信機器が前記第1通信機器を特定する識別子を前記第2通信部を用いて前記第2通信機器に送信し、前記第2通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、前記第2通信機器は前記識別子に基づいて、前記第1通信機器が前記第1通信部を利用して行う通信におけるネットワーク資源の利用可能な範囲を決定してもよい。この通信パラメータ設定方法によると、第

1通信機器を介した不正なネットワーク資源の利用が防止される。

【0022】また、本発明に係る通信パラメータ設定方法は本発明の第1態様において、前記第2通信機器が前記第2通信機器を特定する識別子を前記第2通信部を用いて前記第1通信機器に送信し、前記第1通信機器が前記識別子を前記第2通信部を用いて受信する識別子通信段階を備え、前記第1通信機器は前記識別子を用いて、前記第2通信機器が前記第1通信部を利用して行う通信におけるネットワーク資源の利用可能な範囲を決定してもよい。この通信パラメータ設定方法によると、第2通信機器を介した不正なネットワーク資源の利用が防止される。

【0023】また、上述した課題を解決するために、本発明に係る通信機器は、無線通信が可能な第1通信部と、前記第1通信部とは異なる第2通信部と、記憶部と、前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を前記第2通信部を用いて他の通信機器に送信する制御部とを備えることを特徴としている。

【0024】また、上述した課題を解決するために、本発明に係る他の通信機器は、無線通信が可能な第1通信部と、前記第1通信部とは異なる第2通信部と、記憶部と、この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて受信し、この通信機器と前記第2通信機器が前記第1通信部を利用して通信を行うための通信パラメータを前記案内情報を用いて決定する制御部とを備えることを特徴としている。

【0025】また、上述した課題を解決するために、本発明に係るコンピュータ読み取り可能な記録媒体は、無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、前記第2通信部により他の通信機器との通信が可能になったことを検知させ、前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を前記第2通信部を用いて前記他の通信機器に送信させるプログラムを記録していることを特徴としている。

【0026】また、上述した課題を解決するために、本発明に係る他のコンピュータ読み取り可能な記録媒体は、無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、前記第2通信部により他の通信機器との通信が可能になったことを検知させ、この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することが可能な通信形態に関する案内情報を、前記第2通信部を用いて受信し、この通信機器と前記第2通信機器が前記第1通信部を利用して通信を行うための通信パラメータを前記案

内情報を用いて決定させるプログラムを記録していることを特徴としている。

【0027】また、上述した課題を解決するために、本発明に係るプログラムは、無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、前記第2通信部により他の通信機器との通信が可能になったことを検知させ、前記第1通信部を利用して実行することができる通信形態に関する案内情報を前記第2通信部を用いて前記他の通信機器に送信させることを特徴としている。

【0028】また、上述した課題を解決するために、本発明に係る他のプログラムは、無線通信が可能な第1通信部、前記第1通信部とは異なる第2通信部および記憶部を有する通信機器を制御するコンピュータに、前記第2通信部により他の通信機器との通信が可能になったことを検知させ、この通信機器とは異なる同種の第2通信機器から、前記第2通信機器が前記第1通信部を利用して実行することができる通信形態に関する案内情報を、前記第2通信部を用いて受信し、この通信機器と前記第2通信機器が前記第1通信部を利用して通信を行うための通信パラメータを前記案内情報を用いて決定させることを特徴としている。

【0029】

【発明の実施の形態】次に本発明の望ましい実施形態について説明する。これらの実施形態は本発明の一態様を示すものであってこの発明を限定するものではなく、本発明はその技術的思想の範囲内で任意に変更が可能である。

【0030】〔1〕第1実施形態

〔1.1〕第1実施形態の構成

〔1.1.1〕無線通信システムの構成

本発明の第1実施形態においては、本発明の通信パラメータ設定方法により、互いに未接続の2台の携帯型情報端末が1対1の無線通信を行うことが可能となる。図1に、本発明の第1実施形態における通信パラメータ設定段階の無線通信システムの状態と、通信パラメータ設定後の無線通信システムの状態を示す。なお、本発明の第1実施形態における通信パラメータ設定後に実現される無線通信システムを以下、「無線通信システム1」と呼ぶ。無線通信システム1は携帯型情報端末A1および携帯型情報端末B2により構成される。

〔1.1.2〕携帯型情報端末の構成

図2に、本発明の第1実施形態における携帯型情報端末A1の構成を示す。なお、携帯型情報端末B2の構成は、携帯型情報端末A1と同様であるので、説明を省略する。

【0032】携帯型情報端末A1は、接触型有線通信部14、無線通信部15、操作部16、表示部17および記憶部18と、これらに接続された制御部19とを有し

ている。

【0033】接触型有線通信部14は、他の同種の接触型有線通信部と直接接觸することにより電気的導通状態を作り、制御部19の制御の下で、パラメータ情報などを含む電気信号を送受信する。接触型有線通信部14と同種の接触型有線通信部を持つ全ての携帯型情報端末は同じ有線用通信プロトコルを1つ持つており、携帯型情報端末A1はその有線用通信プロトコルを用いて接触型有線通信部14を介した情報の送受信を行う。

【0034】無線通信部15はアンテナ(図示略)を有しており、このアンテナの受信信号から文字、画像、その他の通信情報を含むベースバンド信号を復調し、このベースバンド信号を制御部19に送信する。また、無線通信部15は、制御部19からベースバンド信号を受信し、このベースバンド信号によってキャリアを変調し、変調した信号をアンテナ(図示略)を介して外部に送信する。無線通信部15は不揮発性メモリ(図示略)を有し、この不揮発性メモリに通信パラメータを記憶し、前記の無線通信を行う際、記憶されている通信パラメータに基づいて通信に用いるチャンネルID、PIN Codeなどを選択する。無線通信部15は複数の無線通信プロトコルに対応しており、それぞれの無線通信プロトコルを使用するための複数の異なるMACアドレスが無線通信部15に割り当てられている。無線通信部15は制御部19の制御の下、これら複数の無線通信プロトコルを使い分ける。

【0035】操作部16はキーパッド(図示略)を有し、ユーザがこのキーパッドのキーを操作すると、操作されたキーに対応した信号を制御部19に送信する。

【0036】表示部17は、液晶パネル(図示略)、駆動回路(図示略)およびビデオRAM(Random Access Memory)(図示略)を有している。制御部19は表示したい文字や図形をピットマップ情報に変換し、このピットマップ情報をビデオRAMに書き込む。駆動回路は一定の時間間隔でビデオRAM内の一画面分のピットマップ情報を読み出し、その情報に基づいて液晶パネルの表示を更新する。

【0037】記憶部18は大容量不揮発性メモリである。記憶部18のデータは、制御部19によって書き込みおよび読み出しが行われる。制御部19は記憶部18の中に一連の情報の集合体としてのファイルを複数作成し、それを管理する。記憶部18は、プロトコル情報ファイル181、暗号鍵情報ファイル182および端末情報ファイル183を記憶している。

【0038】図3はプロトコル情報ファイル181の構成を例示したものである。プロトコル情報ファイル181は、携帯型情報端末A1が利用可能な無線通信プロトコルの数と等しい数のレコードを持っている。各レコードは、携帯型情報端末A1が利用可能な1つの無線通信プロトコルに関する情報の集まりであり、「プロトコ

ル」フィールド、「MACアドレス」フィールド、「パラメータセット」フィールド、および「優先順位」フィールドを持つ。「プロトコル」フィールドは、対象のプロトコルのプロトコル名情報を含む。プロトコル名情報としては、例えば、IEEE802.11b、Bluetooth、IrDA (Infrared Data Association) などがある。「MACアドレス」フィールドは、対象のプロトコルに従って通信を行うときの携帯型情報端末A1のMAC (Media Access Control) アドレスを含む。「パラメータセット」フィールドは複数の子フィールド「パラメータ1」、「パラメータ2」・・・を持ち、各子フィールドは対象のプロトコルのパラメータ情報を1つずつ持つ。パラメータ情報としては、例えばIEEE802.11bのチャネルIDやBluetoothのPIN Codeなどがある。「優先順位」フィールドは、携帯型情報端末A1において利用可能な全ての無線通信プロトコルにおける対象のプロトコルの優先順位を示す正の整数を持つ。この正数値が小さいほど、対象のプロトコルが優先的に利用される。

【0039】図4は暗号鍵情報ファイル182の構成を例示したものである。暗号鍵情報ファイル182は「識別子」アイテムと「暗号鍵」アイテムを持つ。「識別子」アイテムは、携帯型情報端末A1を他の携帯型情報端末から識別するために携帯型情報端末A1に与えられた識別子を含む。この識別子は数字および記号の列であり、他の携帯型情報端末の識別子と同じ値をとることはない。「暗号鍵」アイテムは、無線通信システム1において携帯型情報端末A1が情報を送信する際に、その情報を暗号化するために用いる暗号鍵情報を含む。

【0040】図5は端末情報ファイル183の構成を例示したものである。端末情報ファイル183は、携帯型情報端末A1が今までに本発明の第1実施形態による1対1の無線通信を行った携帯型情報端末に関する情報のファイルである。端末情報ファイル183は、携帯型情報端末A1が今までに無線通信を行った相手の携帯型情報端末の数と等しい数のレコードを持つ。各レコードは「識別子」フィールド、「アクセス権限」フィールド、「暗号鍵」フィールド、「プロトコル」フィールド、および「MACアドレス」フィールドを持つ。「識別子」フィールドは、1対1通信の相手の携帯型情報端末の識別子を含む。「アクセス権限」フィールドは、相手の携帯型情報端末が携帯型情報端末A1のネットワーク資源を利用する場合に、相手の携帯型情報端末に与えられるアクセス権限を表す情報を含む。アクセス権限の例としては、読み取り専用およびフルアクセスがある。あるレコードの「アクセス権限」フィールドが読み取り専用を表している場合、そのレコードの対象である携帯型情報端末が携帯型情報端末A1の持つ共有フォルダ等のネットワーク資源を利用するときには、そのネットワーク資源の参照のみが許可される。一方、あるレコードの「アクセス権限」フィールドがフルアクセスを表している場

合、そのレコードの対象である携帯型情報端末が携帯型情報端末A1のネットワーク資源を利用するときには、そのネットワーク資源の参照、変更および削除が許可される。「暗号鍵」フィールドは、携帯型情報端末A1が相手の携帯型情報端末から暗号化された情報を受信する際、その情報を復号化するために用いる暗号鍵情報を含む。「プロトコル」フィールドは、携帯型情報端末A1が相手の携帯型情報端末と無線通信を行う場合に用いるプロトコル名情報を含む。「MACアドレス」フィールドは、携帯型情報端末A1が相手の携帯型情報端末と無線通信を行う場合に用いる、相手の携帯型情報端末のMACアドレスを含む。

【0041】制御部19は不揮発性メモリ(図示略)を有し、この不揮発性メモリに携帯型情報端末A1の制御を指示するプログラムを記憶し、他の構成要素各部から受信する情報に基づいて、このプログラムに従った処理および構成要素各部の制御を行う。

【0042】[1. 2] 第1実施形態の動作

[1. 2. 1] 通信パラメータ設定段階

20 次に、図6を用いて第1実施形態において無線通信パラメータ設定が行われる際の動作例を説明する。この動作例は、携帯型情報端末A1が、携帯型情報端末B2に対し接続要求を行う場合の動作である。なお、携帯型情報端末A1と携帯型情報端末B2の同種の構成要素を区別するために、各構成要素を特定する符号に“A”および“B”を附加する。以下の動作において、携帯型情報端末A1と携帯型情報端末B2との間の情報の送受信は全て接触型有線通信部14Aおよび接触型有線通信部14Bを介して行われる。

30 【0043】まず、携帯型情報端末A1または携帯型情報端末B2のユーザは、携帯型情報端末A1の接触型有線通信部14Aと携帯型情報端末B2の接触型有線通信部14Bとを直接接触させる(ステップS101)。

【0044】次に、ユーザは携帯型情報端末A1の操作部16Aによって送信指示を入力する。操作部16Aは送信指示信号を制御部19Aに送信する(ステップS102)。制御部19Aはこの信号を受信すると、携帯型情報端末B2に接続要求信号を送信する(ステップS103)。

40 【0045】携帯型情報端末B2の制御部19Bは接続要求信号を受信し、携帯型情報端末B2が携帯型情報端末A1の接続要求に応じることが可能であることを示す接続許可信号を携帯型情報端末A1に送信する(ステップS104)。携帯型情報端末A1の制御部19Aは接続許可信号を受信すると、プロトコル情報ファイル181Aおよび暗号鍵情報ファイル182Aを読み出し、通信パラメータ決定のための案内情報として以下の情報を準備する。

— プロトコル情報ファイル181Aの全レコードの「プロトコル」フィールドおよび「MACアドレス」フィ

ールドの値（以下、「プロトコル・テーブルA」と呼ぶ）

－ 暗号鍵情報ファイル182Aの「識別子」アイテムの値（以下、「ID-A」と呼ぶ）

－ 暗号鍵情報ファイル182Aの「暗号鍵」アイテムの値（以下、「Key-A」と呼ぶ）

上記の情報を準備した後、制御部19Aはこの情報を携帯型情報端末B2に送信する（ステップS105）。

【0046】携帯型情報端末B2の制御部19Bは案内情報として、プロトコル・テーブルA、ID-AおよびKey-Aを受信する。続いて制御部19Bは端末情報ファイル183Bを読み出し、いずれかのレコードの「識別子」フィールドにID-Aと一致する値があるか否かを判定する（ステップS106）。端末情報ファイル183Bのいずれのレコードの「識別子」フィールドにもID-Aと一致する値がない場合、制御部19BはステップS106の判定で「No」を得る。これは携帯型情報端末B2に携帯型情報端末A1が未登録であることを意味する。一方、端末情報ファイル183Bのいずれかのレコードの「識別子」フィールドの値がID-Aと一致する場合、制御部19BはステップS106の判定で「Yes」を得る。これは携帯型情報端末B2に携帯型情報端末A1が登録済みであることを意味する。

【0047】ステップS106の判定において「No」を得た場合、制御部19Bは端末情報ファイル183Bに新しいレコードを追加し、この新たなレコードの「識別子」フィールドの値をID-Aとし、「アクセス権限」フィールドの値を「読み取り専用」とし、「暗号鍵」フィールドの値をKey-Aとする（ステップS107）。

【0048】一方、ステップS106の判定において「Yes」を得た場合、制御部19Bは、端末情報ファイル183Bの「識別子」フィールドの値がID-Aと一致するレコードを検索し、検索されたレコードの「暗号鍵」の値をKey-Aで更新する（ステップS108）。

【0049】ステップS107もしくはステップS108を終えた後、制御部19Bはプロトコル情報ファイル181Bを読み出し、その全レコードの中から、「プロトコル」フィールドに含まれる値が、ステップS106において携帯型情報端末A1から受信したプロトコル・テーブルAのいずれかのレコードの「プロトコル」フィールドの値と一致するレコードを抽出する。プロトコル情報ファイル181Bから複数のレコードが抽出された場合、制御部19Bは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいレコードを選択する。一つのレコードのみが抽出された場合、制御部19Bはそのレコードを選択する。続いて制御部19Bは、選択されたレコードの「プロトコル」フィールドの値（以下、「決定プロトコル1」と呼ぶ）と「MACアドレス」フィールドの値（以下、「MAC-B」と呼ぶ）を取り出す。次に制御部1

9Bはプロトコル・テーブルAの全レコードのうち「プロトコル」フィールドの値が決定プロトコル1と一致するレコードを検索し、検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-A」と呼ぶ）を取り出す。次に制御部19Bは端末情報ファイル183Bを読み出し、全レコードから「識別子」フィールドの値がID-Aと一致するレコードを検索し、検索されたレコードの「プロトコル」フィールドの値を決定プロトコル1で、「MACアドレス」フィールドの値をMAC-Aで更新する（ステップS109）。

【0050】続いて、制御部19Bは、プロトコル情報ファイル181Bを読み出し、その全レコードから「プロトコル」フィールドの値が決定プロトコル1と一致するレコードを検索し、検索されたレコードの「パラメータセット」フィールドの値に基づき、携帯型情報端末A1用のプロトコル・パラメータを決定する（ステップS110）。例えば、決定プロトコル1が“IEEE802.11b”であり、それに対応する「パラメータセット」フィールドが“チャネルID=1”をその値として含んでいれば、制御部19Bは携帯型情報端末A1用のIEEE802.11bのパラメータとして“チャネルID=1”を決定する。以下、ステップS110において決定されたプロトコル・パラメータを「決定パラメータセット1」と呼ぶ。

【0051】次に、制御部19Bは暗号鍵情報ファイル182Bを読み出し、「識別子」アイテムの値（以下、「ID-B」と呼ぶ）および「暗号鍵」アイテムの値（以下、「Key-B」と呼ぶ）を取り出す。続いて、制御部19Bは通信パラメータとして、ID-B、Key-B、決定プロトコル1、MAC-B、および決定パラメータセット1を携帯型情報端末A1に送信する（ステップS111）。

【0052】携帯型情報端末A1の制御部19Aは、ID-B、Key-B決定プロトコル1、MAC-Bおよび決定パラメータセット1を通信パラメータとして受信する。続いて、制御部19Aは端末情報ファイル183Aを読み出し、その全レコードから「識別子」フィールドの値がID-Bと一致するレコードを検索し、検索されたレコードの「暗号鍵」フィールドの値をKey-Bで、「プロトコル」フィールドの値を決定プロトコル1で、「MACアドレス」フィールドの値をMAC-Bで更新する。端末情報ファイル183Aのいずれのレコードの「識別子」フィールドの値もID-Bと一致しない場合は、制御部19Aは端末情報ファイル183Aに新たなレコードを追加し、そのレコードの「識別子」フィールドの値をID-Bとし、「アクセス権限」フィールドの値を「読み取り専用」とし、「暗号鍵」フィールドの値をKey-Bとし、「プロトコル」フィールドの値を決定プロトコル1とし、「MACアドレス」フィールドの値をMAC-Bとする。続いて、制御部19Aは無線通信部15Aに決定プロトコル1および決定パラメータセット1を送信し、無線通信部15Aは不揮発性メモリに記憶している決定プロトコル1に関する

るプロトコル・パラメータを決定パラメータセット1によって更新する。その後、制御部19Aは無線通信パラメータの設定完了のメッセージを表示部17Aに表示する(ステップS112)。

【0053】[1. 2. 2] 暗号鍵を用いた通信方法
ステップS112までの設定作業を終えた後、携帯型情報端末A1が携帯型情報端末B2に情報を送信する場合、まず制御部19Aは暗号鍵情報ファイル182Aを読み出し、携帯型情報端末B2に送信する情報を「暗号鍵」アイテムの値、すなわちKey-Aで暗号化する。続いて制御部19Aは端末情報ファイル183Aを読み出し、「MACアドレス」フィールドの値が情報の送信先のMACアドレス、すなわちMAC-Bと一致するレコードを検索し、検索されたレコードの「プロトコル」フィールドの値が示す通信プロトコルに従って暗号化した情報をフォーマットする。続いて制御部19Aはフォーマットした情報に送信先を示すMAC-Bおよび送信元を示すMAC-Aを付加し、無線通信部15Aを介してその情報を携帯型情報端末B2に送信する。

【0054】また、ステップS112までの設定作業を終えた後、携帯型情報端末A1が携帯型情報端末B2から暗号化された情報を受信する場合、まず制御部19Aは受信した情報から送信元のMACアドレス、すなわちMAC-Bを取り出す。続いて制御部19Aは端末情報ファイル183Aを読み出し、「MACアドレス」フィールドの値がMAC-Bと一致するレコードを検索し、検索されたレコードの「暗号鍵」フィールドの値、すなわちKey-Bを用いて携帯型情報端末A1受信した情報を復号化する。こうして復号化された情報が、携帯型情報端末B2が携帯型情報端末A1のネットワーク資源を利用するすることを要求していることを示す情報を含む場合、制御部19Aは先に読み出したレコードの「アクセス権限」フィールドの値に従い、その要求を許可もしくは拒絶する。

【0055】[1. 3] 第1実施形態の効果

第1実施形態においては、2つの携帯型情報端末が無線通信を行う場合に、ユーザがただそれらの携帯型情報端末の接触型有線通信部を直接接触させることにより、通信に必要となる識別子等の端末情報、無線通信プロトコルに関するパラメータ、暗号鍵等が携帯型情報端末に設定される。従って、携帯型情報端末のユーザがネットワーク技術に関する専門的な知識を持たない場合であっても、簡易に無線通信を開始することができる。

【0056】第1実施形態においては、携帯型情報端末が無線通信システム1にて用いられる無線通信プロトコルが、利用可能な無線通信プロトコルの全てに予め設定されている優先順位に基づき選択される。従って、携帯型情報端末のユーザが無線通信プロトコルに関する技術知識を持たない場合であっても、最適な無線通信プロトコルを用いることできる。

【0057】第1実施形態により実現される無線通信シ

ステム1においては、携帯型情報端末間で通信される情報が暗号化されるため、部外者がその情報を受信した場合でもその情報を解読することができず、情報の漏洩が防止される。

【0058】[1. 4] 第1実施形態の変形例

第1実施形態においては無線通信に必要な通信パラメータを決定する側の通信機器が、通信パラメータを決定しない側の通信機器と同じ携帯型情報端末であるが、通信パラメータを決定する側の通信機器の通信機器は携帯型情報端末に限られない。例えば、通信パラメータを決定する側の通信機器は複数の無線通信機器の通信を中継するアクセスポイントであってもよい。その場合、新たに無線通信を行う携帯型情報端末は本発明の通信パラメータ設定方法により無線通信のための設定を完了した後、アクセスポイントを経由してアクセスポイントに接続している複数の通信機器と通信を行うことができる。

【0059】第1実施形態においては、携帯型情報端末のユーザは携帯型情報端末の接触型有線通信部を他の同種の接触型有線通信部と直接接觸させことにより接続を確立し、携帯型情報端末はこの接続において無線通信システム1における無線通信のための情報の送受信を行っているが、接続の方法はこれに限らない。例えば、携帯型情報端末の有線通信部を相互に通信ケーブルで接続してもよい。また、無線通信システム1における無線通信のための情報を送受信するにあたり、第1実施形態において用いられている接触型有線通信部の代わりに無線通信部が用いられてもよい。この場合には、無線通信システム1において無線通信を行おうとする携帯型情報端末の両方に予め同じ通信パラメータ設定用として無線通信プロトコルを1つ準備しておき、その設定用の無線通信プロトコルを用いて、無線通信システム1において用いられる無線通信プロトコルのための通信パラメータ設定を行う。これにより、直接接続やケーブル接続をする手間が省かれ、より簡易に無線通信に関する通信パラメータ設定を行うことが可能となる。

【0060】第1実施形態においては、ユーザが送信指示の操作を行うことにより接続要求信号が送信されているが、接続要求信号が送信される方法はこれに限られない。例えば、接触型有線通信部が接続された後、タイマにより設定された時間が経過した後に携帯型情報端末の制御部が接続要求信号を送信してもよい。

【0061】第1実施形態においては、無線通信システム1用の独自の識別子が携帯型情報端末に割り当てられているが、識別子は独自のものでなくともよい。例えば、MACアドレスを識別子として用いてもよい。MACアドレスは、通信機器ごとに必ず付加されているため、本発明を用いるにあたり、新たに管理者等が携帯型情報端末ごとに識別子を割り振る必要がなくなる。

【0062】第1実施形態においては、無線通信の通信パラメータ設定完了のメッセージが表示部に表示される

が、通信パラメータ設定完了の通知方法はこれに限らない。例えば、携帯型情報端末が音声出力部を有し、無線通信の設定が完了した場合、携帯型情報端末の制御部が音声出力部を用いて音声により通信パラメータ設定の完了を通知してもよい。

【0063】携帯型情報端末は、第1実施形態における携帯型情報端末の各種制御を制御部に実行させるためのプログラムを、必ずしも予め内部に記憶していなくともよい。例えば、携帯型情報端末がデータ読込部を有し、制御部がこのデータ読込部を用いて前記のプログラムが記録された記録媒体からプログラムを読み取った後に、そのプログラムを実行してもよい。また、携帯型情報端末が電気通信回線により外部の記憶装置のデータにアクセスできる通信部を有し、制御部がこの通信部を用いて前記のプログラムをダウンロードした後に、そのプログラムを実行してもよい。

【0064】第1実施形態において実現される無線通信システム1においては、暗号鍵として共通暗号鍵が用いられているが、本発明において用いられる暗号化の方法は共通鍵方式に限らない。例えば、公開鍵方式により情報を暗号化してもよい。

【0065】【2】第2実施形態

【2. 1】第2実施形態の構成

【2. 1. 1】無線通信システムの構成

本発明の第2実施形態においては、本発明の通信パラメータ設定方法により、第1実施形態と同様に互いに未接続の2台の通信端末が1対1の無線通信を行うことが可能となる。図7に本発明の第2実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の無線通信システムの状態を示す。なお、本発明の第2実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム2」と呼ぶ。無線通信システム2は通信端末C3および通信端末D4により構成される。第1実施形態においては無線通信のための通信パラメータの決定を要求する通信端末と通信パラメータの決定を行う通信端末を決定するために、いずれかの通信端末のユーザが操作部を用いて通信端末に通信パラメータ設定動作の開始の指示を与える必要があったが、第2実施形態においてはその必要はない。通信パラメータ設定段階において、ユーザの介入なしに2台の通信端末のいずれか1つが通信パラメータの決定を要求する役割を選択し、他の1つが通信パラメータの決定を行う役割を選択する。以下、通信パラメータの決定を行う通信端末を「マスタ」、通信パラメータの決定を行わない通信端末を「スレーブ」と呼ぶ。すなわち、マスタは2台の通信端末が無線通信システム2における無線通信を行うために必要な通信パラメータを決定し、その決定された通信パラメータに基づいて自分の通信パラメータの変更を行うと共に、決定された通信パラメータをスレーブに送信する。スレーブはマスタから通信パラメータを受

信し、これに従って自分の通信パラメータを変更する。また、第1実施形態においてはIEEE802.11b等の下位レイヤに関する無線通信プロトコルのパラメータ設定のみが扱われていたが、第2実施形態においてはTCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定も併せて扱う。

【0066】【2. 1. 2】通信端末の構成

図8に、通信端末C3の構成を示す。なお、通信端末D4の構成は通信端末C3の構成と同じであるので、その説明を省略する。

【0067】通信端末C3は有線通信部20、無線通信部21、操作部22、表示部23、制御部24および記憶部25を有している。これらの構成要素はバス26を介して電気的に接続されている。

【0068】有線通信部20、無線通信部21、操作部22、表示部23、制御部24は第1実施形態における携帯型情報端末A1の接触型有線通信部14、無線通信部15、操作部16、表示部17、制御部19とそれぞれ同様であるので、説明を省略する。また、記憶部25の機能も第1実施形態における携帯型情報端末A1の記憶部18と同様であるので、説明を省略する。

【0069】記憶部25は、設定管理情報ファイル251、端末情報ファイル252、自機プロトコル情報ファイル253、他機プロトコル情報ファイル254、決定プロトコル情報ファイル255を記憶し、作業領域256を有している。

【0070】図9は設定管理情報ファイル251の構成を例示したものである。設定管理情報ファイル251は「マスタ・スレーブ」アイテム、「自機識別子」アイテム、「他機識別子」アイテム、「パスワード」アイテム、「共通鍵」アイテム、「設定完了通知フラグ」アイテムを持つ。「マスタ・スレーブ」アイテムは、通信端末C3が無線通信システム2のための無線通信パラメータ設定の際、マスタとして機能するか、スレーブとして機能するかが決定される際に用いられ、“0”、“1”、“2”的いずれかの値をとる。“0”は未設定、“1”はマスタ、“2”はスレーブを意味する。

「自機識別子」アイテムは通信端末C3を他の通信端末から識別するための識別子を含み、この識別子は変更されることはない。なお、識別子は数字および文字の列である。「他機識別子」アイテムは通信端末C3が無線通信システム2において無線通信を行う相手の通信端末の識別子を含む。「パスワード」アイテムは通信端末C3のユーザ以外が通信端末C3を無断で無線通信接続することを防ぐためのパスワードの値を含み、このパスワードの値はユーザが予め任意に設定する。「共通鍵」アイテムは無線通信システム2において通信端末C3が他の通信端末と通信を行う際に通信情報を暗号化および復号化するための暗号鍵情報を含む。「設定完了通知フラグ」アイテムは通信端末C3が無線通信システム2にお

いて無線通信を行う相手の通信端末が、無線通信パラメータ設定を完了したことを確認する為に用いられ、“OFF”、“ON”のいずれかの値をとる。“OFF”は未完了、“ON”は完了を意味する。

【0071】図10は端末情報ファイル252の構成を例示したものである。端末情報ファイル252は、今までに通信端末C3に対する接続を許可された通信端末の数と等しい数のレコードを持ち、各レコードは対象の通信端末の識別子を含む「識別子」フィールドを持つ。

【0072】図11は自機プロトコル情報ファイル253の構成を例示したものである。自機プロトコル情報ファイル253は通信端末C3が利用可能な通信プロトコルの情報からなるファイルである。なお、以下、「プロトコルセット」という言葉を用いる場合、これは下位レイヤのプロトコルと中位レイヤのプロトコルの組み合わせを意味する。プロトコルセットの例としては、“IEEE 802.11b - TCP/IP”、“Bluetooth - NetBEUI”などがある。自機プロトコル情報ファイル253は通信端末C3が利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、各レコードは1つの通信プロトコルセットの情報の集まりであり、「優先順位」フィールド、「MACアドレス」フィールド、「パラメータセット」フィールドを持つ。「優先順位」フィールドは正の整数をとり、この正の整数が小さいほど、対象の通信プロトコルセットの優先順位が高いことを示す。この正の整数は予めユーザもしくは管理者により設定されている。「MACアドレス」フィールドは対象の通信プロトコルセットに割り当てられているMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロトコルセットの名称を示す情報を含む。「パラメータセット」フィールドは複数の子フィールド「パラメータ1」、「パラメータ2」、・・・を持ち、各子フィールドは対象の通信プロトコルセットのパラメータ情報を1つずつ含む。なお、通信プロトコルセットによりパラメータの数が異なるため、「パラメータセット」フィールドの子フィールドの数はあらゆる通信プロトコルセットが必要とするパラメータを含むことができるよう、十分に大きな数が確保されている。

【0073】図12は他機プロトコル情報ファイル254の構成を例示したものである。他機プロトコル情報ファイル254は無線通信システム2において通信端末C3に接続を行う相手の通信端末が利用可能な通信プロトコルセットの情報を含む。他機プロトコル情報ファイル254は相手の通信端末が利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、各レコードは1つの通信プロトコルセットに関する情報の集まりであり、「MACアドレス」フィールドおよび「プロトコルセット」フィールドを持つ。「MACアドレス」は対象の通信プロトコルセットに割り当てられたMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロ

トコルセットの名称を示す情報を含む。

【0074】図13は決定プロトコル情報ファイル255の構成を例示したものである。決定プロトコル情報ファイル255は無線通信システム2において使用される通信プロトコルセットに関する情報を含む。決定プロトコル情報ファイル255は1つのレコードからなり、このレコードは「自機MACアドレス」フィールド、「他機MACアドレス」フィールド、「プロトコルセット」フィールド、「パラメータセット」フィールドを持つ。「自機MACアドレス」フィールドは通信端末C3が対象の通信プロトコルセットを用いて相手の通信端末と通信を行う際の、通信端末C3のMACアドレスを含む。「他機MACアドレス」フィールドは相手の通信端末が対象の通信プロトコルセットを用いて通信端末C3と通信を行う際の、相手の通信端末のMACアドレスを含む。「プロトコルセット」フィールドは対象の通信プロトコルセットの名称を示す情報を含む。「パラメータセット」フィールドは子フィールド「パラメータ1」、「パラメータ2」・・・を持ち、各子フィールドは対象の通信プロトコルセットに関するパラメータを1つずつ含む。

【0075】作業領域256は制御部24が制御処理を行う際にプログラムやデータを一時的に記憶するための領域である。

【0076】[2. 2] 第2実施形態の動作
第2実施形態において、無線通信システム2を実現するための通信パラメータ設定動作および通信パラメータ設定後の通信動作について説明する。通信パラメータ設定は接続認証段階、マスタ・スレーブ決定段階およびパラメータ設定段階から成る。以下の動作例は、通信端末C3と通信端末D4が互いに1対1の無線通信を行うことを可能とする際の動作例である。なお、通信端末C3と通信端末D4の同種の構成要素を区別するために、各構成要素を特定する符号に“C”および“D”を付加する。以下の接続認証段階、マスタ・スレーブ決定段階、およびパラメータ設定段階において、通信端末C3と通信端末D4の間で行われる情報の送受信は全て有線通信部20Cおよび有線通信部20Dを介して行われる。

【0077】[2. 2. 1] 接続認証段階
通信端末C3および通信端末D4はまず、相手の通信端末の認証を行う。図14を用いてその動作説明を行う。以下の動作は通信端末C3と通信端末D4のそれぞれにおいて並行して行われ、通信端末C3と通信端末D4の動作は同じである。従って、ここでは通信端末C3の動作のみを説明する。通信端末D4の動作については、以下の説明における符号“C”と“D”とを入れ替えることにより、その説明が得られる。

【0078】はじめに、通信端末C3または通信端末D4のユーザは、通信端末C3の有線通信部20Cと通信端末D4の有線通信部20Dとを直接接続させる（ステップS201）。

【0079】制御部24Cは、有線通信部20Cを介して他の通信端末との有線接続を検知すると、設定管理情報ファイル251Cを読み出し、「マスタ・スレーブ」アイテムの値を“0”、「設定完了通知フラグ」アイテムの値を“OFF”とする（ステップS202）。

【0080】次に、制御部24Cは設定管理情報ファイル251Cの「自機識別子」アイテムの値（以下、「ID-C」と呼ぶ）を通信端末D4に送信する（ステップS203）。一方、通信端末D4も同様に設定管理情報ファイル251Dの「自機識別子」アイテムの値（以下、「ID-D」と呼ぶ）を通信端末C3に送信する。制御部24CはID-Dを受信し、設定管理情報ファイル251Cの「他機識別子」アイテムの値をID-Dで更新する（ステップS204）。

【0081】続いて、制御部24Cは端末情報ファイル252Cを読み出し、いずれかのレコードの「識別子」フィールドの値がID-Dと一致するか否かを判定する（ステップS205）。通信端末C3が過去に通信端末D4の接続を認証したことがない場合、いずれのレコードの「識別子」フィールドの値もID-Dと一致せず、制御部24CはステップS205の判定で「No」を得る。通信端末C3が過去に通信端末D4の接続を認証したことがある場合、いずれかのレコードの「識別子」フィールドの値がID-Dと一致し、制御部24CはステップS205の判定で「Yes」を得る。

【0082】ステップS205において「Yes」を得た場合、制御部24Cは制御を後述するステップS210に移す。

【0083】ステップS205において「No」を得た場合、制御部24Cはパスワード入力要求のメッセージを表示部23Cに表示する（ステップS206）。このパスワード入力は、通信端末C3が通信端末D4の通信端末C3に対する接続を新たに認証することの確認作業である。通信端末C3のユーザが操作部22Cによってパスワード（以下、このパスワードの値を「入力パスワードC」と呼ぶ）を入力し、制御部24Cが入力パスワードCを受信すると（ステップS207）、制御部24Cは設定管理情報ファイル251Cを読み出し、入力パスワードCが設定管理情報ファイル251Cの「パスワード」アイテムの値（以下、「登録パスワードC」と呼ぶ）と一致するか否かを判定する（ステップS208）。入力パスワードCが登録パスワードCと異なる場合、制御部24CはステップS208の判定で「No」を得る。入力パスワードCが登録パスワードCと同じ場合、制御部24CはステップS208の判定で「Yes」を得る。ステップS208において「No」を得た場合、制御部24Cは制御をステップS206に移す。その後、これら2つのパスワードが一致するまで、ステップS206からステップS208までが繰り返される。なお、上記ステップS206からステップS208

までの動作を以下、「パスワード照合作業」と呼ぶ。

【0084】ステップS208において「Yes」を得た場合、制御部24Cは端末情報ファイル252Cを読み出し、新しいレコードを追加し、そのレコードの「識別子」フィールドの値をID-Dとする（ステップS209）。この作業により、通信端末D4は通信端末C3に新規登録される。制御部24CはステップS209を終えると、制御をステップS210に移す。なお、上記ステップS205からステップS209までの動作を以下、「識別子登録作業」と呼ぶ。

【0085】[2. 2. 2] マスタ・スレーブ決定段階 上述の接続認証段階を終えた後、通信端末C3および通信端末D4はどちらの通信端末がマスタとなり、どちらの通信端末がスレーブとなるかを決定する。図15を用いてその動作説明を行う。以下の動作は通信端末C3と通信端末D4のそれぞれにおいて並行して行われ、通信端末C3と通信端末D4とは同じ動作をする。従って、ここでは通信端末C3の動作のみを説明する。通信端末D4の動作については、以下の説明における符号CとDとを入れ替えることにより、その説明が得られる。

【0086】制御部24Cは通信端末D4の接続認証を終えると、設定管理情報ファイル251Cを読み出し、「自機識別子」アイテムの値、すなわちID-Cと、「他機識別子」アイテムの値、すなわちID-Dを用いた演算により、通信端末C3がマスタとして機能すべきか否かを判定する（ステップS210）。この判定ための演算の例として、ID-CとID-Dの2進数表現による値の和をとり、その和が偶数の場合は識別子が大きい方の通信端末をマスタとし、その和が奇数の場合は識別子が小さい方の通信端末をマスタとする方法がある。ただし、この方法に限らず、通信端末C3と通信端末D4のいずれがマスタとして機能すべきかを一意に決定可能な方法であれば何であってもよい。通信端末C3がマスタとして機能すべき場合、制御部24CはステップS210の判定で「Yes」を得る。通信端末D4がマスタとして機能すべき場合、制御部24CはステップS210の判定で「No」を得る。

【0087】ここで、以下のステップにおいて通信端末D4が通信端末C3に対して行う割り込み処理要求について説明する。通信端末C3はステップS210の判定に基づき、下記のステップS213もしくはステップS214において、通信端末D4に対しマスタ設定要求もしくはスレーブ設定要求を割り込み要求として送信する。同様に、通信端末D4は通信端末C3に対しマスタ設定要求もしくはスレーブ設定要求を割り込み要求として送信する。通信端末C3の制御部24Cはマスタ設定要求を受信すると、それまでの処理を一時停止し、設定管理情報ファイル251Cを読み出し、「マスタ・スレーブ」アイテムの値を“1”で更新した後、一時停止した前記処理を再開する。同様に、制御部24Cはスレ

ブ設定要求を受信すると、それまでの処理を一時停止し、設定管理情報ファイル251Cを読み出し、「マスタ・スレーブ」アイテムの値を“2”で更新した後、一時停止した前記処理を再開する。これらの割り込み処理要求の送信はマスタ・スレーブ決定段階においてのみ行われるが、受信はマスタ・スレーブ決定段階のみでなく、接続認証段階においても行われる可能性がある。以上が割り込み処理要求の説明である。

【0088】ステップS210において「Yes」を得た場合、制御部24Cは設定管理情報ファイル251Cを読み出し、「マスタ・スレーブ」アイテムの値を取り出す（ステップS211）。この時点で、通信端末C3が既に通信端末D4からマスタ設定要求を受信している場合、制御部24CはステップS211で「1」を得る。この時点で、通信端末C3がまだ通信端末D4からマスタ設定要求を受信していない場合、制御部24CはステップS211で「0」を得る。通信端末C3と通信端末D4は同じ演算を行うので、この場合、通信端末D4が通信端末C3に対しスレーブ設定要求を送信することはなく、従って制御部24CはステップS211で「2」を得ることはない。

【0089】ステップS211において「0」を得た場合、制御部24Cは予め定められた短時間、例えば1秒間だけ待機した後、ステップS211に制御を戻す（ステップS212）。この動作はステップS211において、「マスタ・スレーブ」の値が“0”である限り繰り返される。この間、通信端末C3は通信端末D4から送信されてくるべきマスタ設定要求の待ち状態にある。

【0090】ステップS211において「1」を得た場合、制御部24Cは通信端末D4に対し、スレーブ設定要求を送信する（ステップS213）。これは通信端末C3が通信端末D4の行った演算処理と同じ結果を得たことの確認通知の意味を持つ。制御部24CはステップS213を終えると、後述するステップS219に制御を移す。

【0091】ステップS210において「No」を得た場合、制御部24Cは通信端末D4に対し、マスタ設定要求を送信する（ステップS214）。これは通信端末C3が自分の行った演算処理の結果を通信端末D4に通知し、通信端末D4にその結果の確認を要求する意味を持つ。

【0092】ステップS214において通信端末D4にマスタ設定要求を送信した後、制御部24Cは設定管理情報ファイル251Cを読み出し、「マスタ・スレーブ」アイテムの値を取り出す（ステップS215）。この時点で、通信端末C3が既に通信端末D4からスレーブ設定通知を受信している場合、制御部24CはステップS215で「2」を得る。この時点で、通信端末C3がまだ通信端末D4からスレーブ設定要求を受信していない場合、制御部24CはステップS215で「0」を得る。

得る。通信端末C3と通信端末D4は同じ演算を行うので、この場合、通信端末D4が通信端末C3に対しマスタ設定要求を送信することなく、従って制御部24CはステップS215で「1」を得ることはない。

【0093】ステップS215において「0」を得た場合、制御部24Cは予め定められた短時間、例えば1秒間だけ待機した後、ステップS215に制御を戻す（ステップS216）。この動作はステップS215において、「マスタ・スレーブ」の値が“0”である限り繰り返される。この間、通信端末C3は通信端末D4から送信されてくるべきスレーブ設定要求の待ち状態にある。

【0094】ステップS215において「2」を得た場合、制御部24Cは後述するステップS217に制御を移す。

【0095】[2. 2. 3] パラメータ設定段階

上述のマスタ・スレーブ決定段階を終えた後、通信端末C3および通信端末D4は無線通信のためのパラメータ設定を行う。図16および図17を用いてその動作説明を行う。

【0096】なお、以下においてはマスタとして機能する通信端末Mとスレーブとして機能する通信端末Sの動作について説明を行う。従って、通信端末C3がマスタの場合には符号MをCと入れ替えることにより、また通信端末C3がスレーブの場合には符号SをCと入れ替えることにより、その説明が得られる。通信端末Dについても同様である。なお、通信端末Mと通信端末Sの同種の構成要素を区別するために、各構成要素を特定する符号に“M”および“S”を附加する。

【0097】まず、通信端末Sの制御部24Sは、任意の暗号鍵を生成し、設定管理情報ファイル251Sを読み出し、「共通鍵」アイテムの値を生成した暗号鍵（以下、「Key-2」と呼ぶ）で更新する（ステップS217）。この暗号鍵は文字、数字および記号の列であり、乱数関数により生成される。乱数関数については既に多くの既知のものがあるため、ここでの説明は省略する。

【0098】次に制御部24Sは自機プロトコル情報ファイル253Sを読み出し、全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値（以下、「プロトコルセット・テーブルS」と呼ぶ）を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・テーブルSは通信端末Sが無線通信部21Sを用いた通信を行う際に利用可能なプロトコルセットに関する案内情報である。統いて制御部24Sはプロトコルセット・テーブルSと、ステップS217で生成したKey-2を通信端末Mに送信する（ステップS218）。通信端末Mの制御部24Mはプロトコルセット・テーブルSおよびKey-2を受信すると、他機プロトコル情報ファイル254Mを読み出し、他機プロトコル情報ファイル254Mの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールド

の値を、プロトコルセット・テーブルSの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値で更新する。更に、設定管理情報ファイル251Mを読み出し、「共通鍵」アイテムの値をKey-2で更新する（ステップS219）。

【0099】次に制御部24Mは自機プロトコル情報ファイル253Mおよび他機プロトコル情報ファイル254Mを読み出し、それぞれの「プロトコルセット」フィールドに共通する値が存在するか否かの判定をする（ステップS220）。自機プロトコル情報ファイル253Mの「プロトコルセット」フィールドと他機プロトコル情報ファイル254Mの「プロトコルセット」フィールドの両方に同じプロトコルセットの名称を示す値が存在する場合には、制御部24MはステップS220で「Yes」を得る。同じプロトコルセットが存在しない場合には、制御部24MはステップS220で「No」を得る。

【0100】ステップS220で「No」を得ると、制御部24Mは通信不成立通知を通信端末Sに送信する。また制御部24Mは、無線通信の設定が不可能であることを通知するメッセージを表示部23Mに表示する（ステップS221）。このステップを経た場合、制御部24Mの動作は終了する。通信端末Sの制御部24Sは、通信端末Mより通信不成立通知を受信すると、無線通信の設定が不可能であることを通知するメッセージを表示部23Sに表示する（ステップS222）。このステップを経た場合、制御部24Sの動作は終了する。なお、ステップS220からステップS222までの動作を以下、「通信可能確認作業」と呼ぶ。

【0101】ステップS220で「Yes」を得た場合、制御部24Mは、自機プロトコル情報ファイル253Mの全てのレコードの中から、「プロトコルセット」フィールドに含まれる値が他機プロトコル情報ファイル254Mのいずれかのレコードの「プロトコルセット」フィールドの値と一致するレコードを抽出する。自機プロトコル情報ファイル253Mから複数のレコードが抽出された場合、制御部24Mは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいレコードを選択する。一つのレコードのみが抽出された場合、制御部24Mはそのレコードを選択する。次に、制御部24Mは決定プロトコル情報ファイル255Mを読み出し、その唯一のレコードの「自機MACアドレス」フィールドの値を選択されたレコードの「MACアドレス」フィールドの値（以下、「MAC-M」と呼ぶ）で、「プロトコルセット」フィールドの値を選択されたレコードの「プロトコルセット」フィールドの値（以下、「決定プロトコルセット2」と呼ぶ）で更新する。続いて、制御部24Mは他機プロトコル情報ファイル254Mの全てのレコードの中から、「プロトコルセット」フィールドの値が決定プロトコルセット

2と一致するレコードを検索し、決定プロトコル情報ファイル255Mの「他機MACアドレス」フィールドの値を検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-S」と呼ぶ）で更新する（ステップS223）。

【0102】次に、制御部24MはステップS223において選択された自機プロトコル情報ファイル253Mのレコードの「パラメータセット」フィールドの値に基づいて、通信端末Sが通信端末Mと決定プロトコルセット2の示すプロトコルセットを用いて無線通信を行うために変更の必要な通信パラメータの値を決定する（ステップS224）。以下、通信端末M用のパラメータセットを「パラメータセットM」、通信端末S用のパラメータセットを「パラメータセットS」と呼ぶ。

【0103】ステップS224におけるパラメータセットの決定動作について、例を挙げて説明する。例えば、今、決定プロトコルセット2が“IEEE802.11b - TCP/IP”を示し、自機プロトコル情報ファイル253Mの「プロトコルセット」の値が“IEEE802.11b - TCP/IP”を示すレコードの「パラメータセット」フィールドの値が、

パラメータ1 “IEEE802.11b: モード=Infrastructure”

パラメータ2 “IEEE802.11b: チャンネルID=3”

パラメータ3 “IPアドレス / サブネットマスク=192.168.0.220 / 255.255.255.0”

であったとする。この場合、制御部24MはパラメータセットMとして、

パラメータ1 “IEEE802.11b: モード=Ad Hoc”

30 パラメータ2 “IEEE802.11b: チャンネルID=5”を決定する。また、パラメータセットSとして、

パラメータ1 “IEEE802.11b: モード=Ad Hoc”

パラメータ2 “IEEE802.11b: チャンネルID=5”

パラメータ3 “IPアドレス / サブネットマスク=192.168.0.221 / 255.255.255.0”

を決定する。ここで、InfrastructureモードはIEEE802.11bにおいて規定されているアクセスポイントを中継する通信形態を、またAd HocモードはIEEE802.11bにおいて規定されているピア・トゥ・ピアの通信形態を指す。

【0104】通信端末Mは、元の設定ではIEEE802.11において、Infrastructureモードを用いている。無線通信システム2においては1対1の無線通信が行われることから、制御部24MはIEEE802.11bの通信モードとしてAd Hocモードを選定している。また、通信端末Mは元の設定ではIEEE802.11bのチャンネルIDとして3を用いている。チャンネルID3は通信端末Mが元の設定で属していた無線通信網における周波数であり、無線通信システム2においてこれを用いると周波数の衝突が生ずるので、制御部24Mは3以外の未使用なチャンネルIDとして5を選定している。また、TCP/IPのパラメータに関し

ては、通信端末Mは元の設定ではIPアドレスとして192.168.0.220、サブネットマスクとして255.255.255.0を用いている。ここで通信端末MのIPアドレスおよびサブネットマスクを変更する必要はないので、通信端末M用のパラメータセットにはIPアドレス / サブネットマスクに関するパラメータが含まれていない。一方、通信端末SのIPアドレスおよびサブネットマスクは通信端末Mと同じネットワークに属し、異なるアドレスを示すものである必要があるので、制御部24Mは通信端末S用のパラメータとして、IPアドレスとして192.168.0.221、またサブネットマスクとして255.255.255.0を選定している。

【0105】ステップS224においてパラメータセットMおよびパラメータセットSを決定した後、まず制御部24Mは決定プロトコル情報ファイル255Mを読み出し、その唯一のレコードの「パラメータセット」フィールドの値をパラメータセットMで更新する。続いて、制御部24Mはそのレコードの「自機MACアドレス」フィールドの値、すなわちMAC-M、および「プロトコルセット」フィールドの値、すなわち決定プロトコルセット2を取り出し、MAC-M、決定プロトコルセット2およびパラメータセットSを通信端末Sに送信する（ステップS225）。これらの情報は通信端末Sが無線通信部21Sを用いて通信端末Mと通信を行うための通信パラメータである。

【0106】制御部24SはMAC-M、決定プロトコルセット2およびパラメータセットSを通信端末Mから受信すると、決定プロトコル情報ファイル255Sを読み出し、唯一のレコードの「他機MACアドレス」フィールドの値をMAC-M、「プロトコルセット」フィールドの値を決定プロトコルセット2、「パラメータセット」フィールドの値をパラメータセットSで更新する。続いて、制御部24Sは自機プロトコル情報ファイル253Sを読み出し、その全レコードから「プロトコルセット」フィールドの値が決定プロトコルセット2と一致するレコードを検索し、検索されたレコードの「MACアドレス」フィールドの値、すなわちMAC-Sを取りだし、決定プロトコル情報ファイル255Sの唯一のレコードの「自機MACアドレス」フィールドの値をMAC-Sで更新する（ステップS226）。

【0107】以下の動作は通信端末Mと通信端末Sのそれれにおいて並行して行われ、通信端末Mと通信端末Sとは同じ動作をする。従って、ここでは通信端末Mの動作のみを説明する。通信端末Sの動作については、以下の説明における符号MとSとを入れ替えることにより、その説明が得られる。

【0108】制御部24Mは決定プロトコル情報ファイル255Mを読み出し、その唯一のレコードの「プロトコルセット」フィールドの値、すなわち決定プロトコルセット2および「パラメータセット」フィールドの値、

すなわちパラメータセットMを無線通信部21Mに送信する。無線通信部21Mは決定プロトコルセット2およびパラメータセットMを受信すると、不揮発性メモリに記憶されている、決定プロトコルセット2が示す通信プロトコルセットに関する通信パラメータを、パラメータセットMに基づいて変更する。なお、この変更を終えた無線通信部21Mは、設定終了を制御部24Mに通知する（ステップS227）。

【0109】設定終了の通知を無線通信部21Mより受信すると、制御部24Mは設定完了通知を通信端末Sに送信する（ステップS228）。

【0110】ここで、以下の動作で通信端末Sが通信端末Mに対して行う割り込み処理要求について説明する。上述のとおり、通信端末MはステップS228において、通信端末Sに対し設定完了通知を送信するが、同様に通信端末Sは通信端末Mに対し設定完了通知を送信する。この設定完了通知を受信すると、制御部24Mは、それまでの処理を一時停止し、設定管理情報ファイル251Mを読み出し、「設定完了通知フラグ」アイテムの値を“ON”で更新した後、一時停止した前記処理を再開する。

【0111】ステップS228において設定完了通知を送信した後、制御部24Mは設定管理情報ファイル251Mを読み出し、「設定完了通知フラグ」アイテムの値が“ON”であるか否かを判定する（ステップS229）。この時点で、通信端末Mが通信端末Sより既に設定完了通知を受信している場合、制御部24MはステップS229の判定結果として「Yes」を得る。通信端末Mが通信端末Sより設定完了通知を受信していない場合、制御部24MはステップS229の判定結果として「No」を得る。ステップS229において、「No」を得た場合、制御部24Mは予め定められた短時間、例えば1秒間だけ待機した後、ステップS229に制御を戻す（ステップS230）。この動作はステップS229において、「設定完了通知フラグ」の値が“OFF”である限り繰り返される。この間、通信端末Mは通信端末Sから送信されてくるべき設定完了通知の待ち状態にある。

【0112】ステップS229において、「Yes」を得た場合、制御部24Mは、無線通信の設定が完了したこと通知するメッセージを表示部23Mに表示する（ステップS231）。

【0113】ステップS231において表示されたメッセージにより、無線通信のパラメータ設定が完了したこと確認した通信端末Mおよび通信端末Sのユーザは、有線通信部20Mと有線通信部20Sとの接続を解除できる。以上の動作により、通信端末Mおよび通信端末Sは決定プロトコルセット2を用いて、無線通信部21Mおよび無線通信部21Sを用いた1対1の無線通信を行うことができるようになる。

【0114】[2. 2. 4] 共通鍵を用いた通信方法
上記の通信パラメータ設定段階を終えた後、通信端末C3および通信端末D4は無線通信システム2における1対1の無線通信を行う際、その通信情報を共通鍵を用いて暗号化および復号化する。以下、その通信動作を説明する。なお、以下は通信端末C3が通信端末D4に情報を送信する場合について説明するが、通信端末C3および通信端末D4の立場が逆となってもよい。

【0115】通信端末C3が通信端末D4に情報を送信する必要が生じると、まず制御部24Cは決定プロトコル情報ファイル255Cを読み出し、送信先である通信端末D4のMACアドレス（以下、「MAC-D」と呼ぶ）を、決定プロトコル情報ファイル255Cの唯一のレコードの「他機MACアドレス」フィールドの値と比較する。この比較は情報の送信先が無線通信システム2において確立されている1対1の無線通信の相手の通信端末であることの確認作業である。この比較において2つの値が一致すると、制御部24Cは設定管理情報ファイル251Cを読み出し、「共通鍵」アイテムの値、すなわちKey-2で通信端末D4に送信する情報を暗号化する。次に制御部24Cは決定プロトコル情報ファイル255Cの唯一のレコードの「プロトコルセット」フィールドの値が示す通信プロトコルセットに従って、暗号化した情報をフォーマットする。続いて制御部24Cは決定プロトコル情報ファイル255Cの唯一のレコードの「自機MACアドレス」フィールドの値（以下、「MAC-C」と呼ぶ）を取り出し、フォーマットした情報に送信先を示すMAC-Dおよび送信元を示すMAC-Cを付加し、無線通信部21Cを介してその情報を通信端末D4に送信する。

【0116】通信端末D4の制御部24Dは無線通信部21Dを介して、通信端末C3から暗号化された情報を受信すると、まず制御部24Dは受信した情報から送信元のMACアドレス、すなわちMAC-Cを取り出す。続いて制御部24Dは決定プロトコル情報ファイル255Dを読み出し、MAC-Cを、その唯一のレコードの「他機MACアドレス」フィールドの値と比較する。この比較は情報の送信元が無線通信システム2において確立されている1対1の無線通信の相手の通信機器であることの確認作業である。この比較において2つの値が一致すると、制御部24Dは設定管理情報ファイル251Dを読み出し、「共通鍵」アイテムの値、すなわちKey-2で受信した情報を復号化する。

【0117】[2. 3] 第2実施形態の効果

第2実施形態においては、各通信端末のユーザは通信端末の有線通信部を直接接触させる、という直感的に理解可能な方法によって無線通信のパラメータ設定を行うことができ、その他、アプリケーションソフトを起動する等の手間を要しない。これはユーザにとっての通信パラメータ設定準備作業を大幅に軽減する。

【0118】第2実施形態において、通信パラメータ設

定時に無線通信のユーザが行うべきことは、ユーザが自分で任意に登録したパスワードの入力のみである。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。なお、この通信パラメータ設定においては、いずれかの通信端末において優先度が高く設定されている通信プロトコルが自動的に選択されるため、設定が自動化されたために不適当な通信プロトコルが選択されて通信効率が落ちる、といったことはない。

【0119】第2実施形態において実現される無線通信システム2においては、通信端末間の情報は全て暗号化されるため、部外者の無線機器がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。暗号化は既によく知られた技術であるが、共通鍵を用いる方法は公開鍵を用いる方法と比べてスピードの速い情報の暗号化および復号化が可能である一方で、共通鍵の盗用の危険性がある。しかしながら、無線通信システム2においては通信端末が直接接続されることによりこの共通鍵が受け渡されるため、効率的な共通鍵による暗号技術を安全に用いることができる。

【0120】[3] 第3実施形態

[3. 1] 第3実施形態の構成

[3. 1. 1] 無線通信システムの構成

本発明の第3実施形態においては、本発明の通信パラメータ設定方法により、複数の通信機器を含む既に稼働している無線通信網に対し新たに通信機器が無線接続し、この新たに参加する通信機器がこの無線通信網に含まれる複数の通信機器と通信を行うことが可能となる。図18に本発明の第3実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の状態を示す。本発明の第3実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム3」と呼ぶ。第3実施形態においては、通信端末F6、通信端末G7および通信端末H8が既に無線通信で互いに接続されており、通信端末E5が通信端末F6とケーブルにより接続されることにより、新たに通信端末E5が通信端末F6、通信端末G7および通信端末H8と無線通信を行うことができるようになる。第3実施形態においては、通信端末E5のユーザが通信端末E5の操作部を用いて通信パラメータ設定の開始指示を行うことにより、通信端末E5が無線通信システム3における通信パラメータの決定を要求する側の通信機器、通信端末F6が通信パラメータの決定を行う側の通信機器となる。これにより、通信端末F6は通信端末E5が無線通信システム3における無線通信を行うための通信パラメータを決定し、その決定された通信パラメータを通信端末E5に送信する。通信端末E5は通信端末F6から通信パラメータを受信し、受信した通信パラメータに基づいて自分の通信パラメータを変更する。なお、第3実施形態においては第2実施形態と同様に、TCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定

も併せて行う。

【0121】[3. 1. 2] 通信端末の構成

【3. 1. 2. 1】有線通信部を有する通信端末の構成
第3実施形態において、通信端末E5は通信端末F6とケーブルで接続されることにより、他の通信端末と無線通信が可能となる。図19を用いて通信端末E5の構成を説明する。なお、通信端末F6の構成は通信端末E5のものと同じであるので、通信端末F6の説明は省略する。

【0122】通信端末E5は有線通信部27、無線通信部28、操作部29、表示部30、制御部31および記憶部32を備えている。これらの構成要素はバス33を介して電気的に接続されている。

【0123】無線通信部28、操作部29、表示部30、制御部31の機能および構成は第2実施形態における通信端末C3の無線通信部21、操作部22、表示部23、制御部24のものとそれ同様であるので、説明を省略する。また、記憶部32の機能も第2実施形態における通信端末C3の記憶部25のものと同様であるので、説明を省略する。

【0124】有線通信部27の機能は第2実施形態における通信端末C3の有線通信部20と同様であるが、その形状は直接接続ではなく、ケーブル接続が可能な形状をしている。

【0125】記憶部32は、設定管理情報ファイル321、端末情報ファイル322、自機プロトコル情報ファイル323、他機プロトコル情報ファイル324、決定プロトコル情報ファイル325、識別子情報ファイル326および公開鍵情報ファイル327を記憶し、また作業領域328を有している。

【0126】端末情報ファイル322、他機プロトコル情報ファイル324および作業領域328の構成に関しては第2実施形態における通信端末C3の端末情報ファイル252、他機プロトコル情報ファイル254および作業領域256のものと同様であるので、説明を省略する。

【0127】図20は設定管理情報ファイル321の構成を例示したものである。設定管理情報ファイル321は「自機識別子」アイテム、「パスワード」アイテム、「秘密鍵」アイテム、「公開鍵」アイテムを持つ。「自機識別子」アイテムおよび「パスワード」アイテムの機能は第2実施形態における通信端末C3の設定管理情報ファイル251のものと同様である。「秘密鍵」アイテムは、無線通信システム3において通信端末E5が通信端末E5以外の通信端末から暗号化された通信情報を受信する際、その通信情報を復号化するための暗号鍵情報を含む。「公開鍵」アイテムは、無線通信システム3において通信端末E5以外の通信端末が通信端末E5に対し情報を送信する際、その通信情報を暗号化するための暗号鍵情報を含む。「秘密鍵」アイテムの値と「公開

鍵」アイテムの値は1対をなし、「公開鍵」アイテムの値によって暗号化された情報は「秘密鍵」アイテムの値によってのみ、復号化される。

【0128】図21は自機プロトコル情報ファイル323の構成を例示したものである。自機プロトコル情報ファイル323の構成は第2実施形態における通信端末C3の自機プロトコル情報ファイル253とほぼ同様であるが、「優先順位」フィールドは不要なため、持っていない。

【0129】図22は決定プロトコル情報ファイル325の構成を例示したものである。決定プロトコル情報ファイル325の構成は第2実施形態における通信端末C3の決定プロトコル情報ファイル255とほぼ同様であるが、通信端末E5と通信端末F6とが共通して利用可能な通信プロトコルセットの数と等しい数のレコードを持ち、それぞれのレコードは1つの通信プロトコルセットに対応した情報の集まりである。

【0130】図23は識別子情報ファイル326の構成を例示したものである。識別子情報ファイル326は今までに通信端末E5が無線通信システム3における通信を行ったことがある相手の通信端末のMACアドレスおよび識別子を記憶する。識別子情報ファイル326は今までに通信端末E5が無線通信システム3における通信を行ったことがある通信端末のMACアドレスの数と等しい数のレコードを持ち、各レコードは「MACアドレス」フィールドと「識別子」フィールドを持つ。「MACアドレス」フィールドは対象の通信端末のMACアドレスを含み、「識別子」フィールドは対象の通信端末の識別子を含む。1つの通信端末が複数のMACアドレスを持つ場合、それら複数のMACアドレスに対応するレコードにおける「識別子」フィールドの値は等しい。

【0131】図24は公開鍵情報ファイル327の構成を例示したものである。公開鍵情報ファイル327は今までに通信端末E5が無線通信システム3における通信を行ったことがある相手の通信端末の公開鍵情報を記憶する。公開鍵情報ファイル327は今までに通信端末E5が無線通信システム3における通信を行ったことがある通信端末の数と等しい数のレコードを持ち、各レコードは「識別子」フィールドと「公開鍵」フィールドを持つ。「識別子」フィールドは対象の通信端末の識別子を含み、「公開鍵」フィールドは対象の通信端末の公開鍵情報を含む。

【0132】[3. 1. 2. 2] 有線通信部を有さない通信端末の構成

第3実施形態において、通信端末G7および通信端末H8は通信端末E5とケーブルで接続されることなく、それらの構成は通信端末E5および通信端末F6の構成と異なる。図25を用いて通信端末G7の構成を説明する。通信端末H8の構成は通信端末G7のものと同じであるので、通信端末H8の説明は省略する。

【0133】通信端末G 7は無線通信部3 4、操作部3 5、表示部3 6、制御部3 7および記憶部3 8を備えている。これらの構成要素はバス3 9を介して電気的に接続されている。

【0134】無線通信部3 4、操作部3 5、表示部3 6、制御部3 7の機能および構成は第2実施形態における通信端末C 3の無線通信部2 1、操作部2 2、表示部2 3、制御部2 4のものと同様であるので、説明を省略する。また、記憶部3 8の機能も第2実施形態における通信端末C 3の記憶部2 5のものと同様であるので、説明を省略する。

【0135】記憶部3 8は、設定管理情報ファイル3 8 1、識別子情報ファイル3 8 2および公開鍵情報ファイル3 8 3を記憶し、また作業領域3 8 4を有している。

【0136】識別子情報ファイル3 8 2および公開鍵情報ファイル3 8 3の構成に関しては通信端末E 5の識別子情報ファイル3 2 6および公開鍵情報ファイル3 2 7のものと同様であるので、説明を省略する。また、作業領域3 2 8の構成に関しては、第2実施形態における通信端末C 3の作業領域2 5 6のものと同様であるので、説明を省略する。

【0137】図2 6は設定管理情報ファイル3 8 1の構成を例示したものである。設定管理情報ファイル3 8 1は「自機識別子」アイテム、「秘密鍵」アイテムおよび「公開鍵」アイテムを持つ。「自機識別子」アイテムの機能は第2実施形態における通信端末C 3の設定管理情報ファイル2 5 1のものと同様である。「秘密鍵」アイテムおよび「公開鍵」アイテムの機能は通信端末E 5の設定管理情報ファイル3 2 1のものと同様である。

【0138】[3. 2] 第3実施形態の動作

第3実施形態において、無線通信システム3を実現するための通信パラメータ設定動作および通信パラメータ設定後の通信動作を説明する。通信パラメータ設定は接続認証段階およびパラメータ設定段階から成る。以下の説明において、通信端末E 5、通信端末F 6、通信端末G 7の同種の構成要素を区別するために、各構成要素を特定する符号に“E”、“F”、“G”を付加する。なお、以下の接続認証段階およびパラメータ設定段階において、通信端末E 5と通信端末F 6の間で行われる情報の送受信は全て有線通信部2 7 Eおよび有線通信部2 7 Fを介して行われる。

【0139】[3. 2. 1] 接続認証段階

まず、通信端末F 6は通信端末E 5の接続要求に応じて、通信端末E 5が自分の通信端末に接続することの認証作業を行う。以下、図2 7を用いてその動作説明を行う。

【0140】はじめに、通信端末E 5および通信端末F 6のユーザは接続ケーブルの一端をそれぞれ有線通信部2 7 Eおよび有線通信部2 7 Fに接続する。有線通信部2 7 Eと有線通信部2 7 Fが接続ケーブルによって電気

的に導通すると、制御部3 1 Eおよび制御部3 1 Fは有線通信部2 7 Eおよび有線通信部2 7 Fを介してこの接続を検知する(ステップS 3 0 1)。

【0141】制御部3 1 Eは次にパスワード照合作業を行う。パスワード照合作業は第2実施形態におけるステップS 2 0 6からステップS 2 0 8とほぼ同様であるので、詳細な説明を省略する(ステップS 3 0 2からステップS 3 0 4)。ただし、ステップS 3 0 2において表示部3 0 Eに表示されるメッセージは、新たに無線通信網に参加する通信端末側のユーザのみ、パスワード入力を行うように指示する。このパスワード入力は、正しいユーザが通信端末E 5の無線通信網への接続を試みていることを確認すると同時に、通信端末E 5の相手の通信端末が以下の動作において通信パラメータの決定を行うことを通信端末E 5に指示するための動作である。通信端末F 6の制御部3 1 Fは、ステップS 3 0 1に続き制御部3 1 Eと同様のパスワード入力要求のメッセージ表示(ステップS 3 0 2)を行うが、通信端末F 6は新たに無線通信網に参加する通信端末ではないので、通信端末F 6のユーザはパスワードを入力せず、従って制御部3 1 Fはパスワード照合作業のステップS 3 0 3およびステップS 3 0 4を行わない。

【0142】ステップS 3 0 4において、2つのパスワードが一致した場合、制御部3 1 Eは設定管理情報ファイル3 2 1 Eおよび自機プロトコル情報ファイル3 2 3 Eを読み出し、まず設定管理情報ファイル3 2 1 Eの「自機識別子」アイテムの値(以下、「ID-E」と呼ぶ)を取り出す。次に制御部3 1 Eは自機プロトコル情報ファイル3 2 3 Eの全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値(以下、「プロトコルセット・テーブルE」と呼ぶ)を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・リストEは通信端末E 5が無線通信部2 8 Eを用いた通信を行う際に利用可能なプロトコルに関する案内情報である。次に、制御部3 1 EはID-Eおよびプロトコルセット・テーブルEを通信端末F 6に送信する(ステップS 3 0 5)。ステップS 3 0 5を終えた制御部3 1 Eは制御を後述のステップS 3 1 4に移す。

【0143】通信端末F 6の制御部3 1 FはID-Eおよびプロトコルセット・テーブルEを受信すると、まず設定管理情報ファイル3 2 1 Fを読み出し、「他機識別子」アイテムの値をID-Eで更新する。続いて、制御部3 1 Fは他機プロトコル情報ファイル3 2 4 Fを読み出し、その各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値をプロトコルセット・テーブルEの各レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値でそれぞれ更新する(ステップS 3 0 6)。

【0144】通信端末F 6は次に識別子登録作業を行う。識別子登録作業は第2実施形態におけるステップS

205からステップS209と同様であるので、説明を省略する（ステップS307からステップS311）。ステップS311を終えた制御部31Fは制御を後述のステップS312に移す。

【0145】[3. 2. 2] パラメータ設定段階
上記の接続認証段階を終えた後、通信端末F6は通信端末E5が無線通信のために必要とする通信パラメータの決定を行い、通信端末E5は通信端末F6により決定されたパラメータに従い、パラメータの設定を行う。以下、図28を用いてその動作説明を行う。

【0146】まず、通信端末E5および通信端末F6は通信可能確認作業を行う。通信可能確認作業は第2実施形態におけるステップS220からステップS222と同様であるので、説明を省略する（ステップS312からステップS314）。ただし、この通信可能確認作業において、通信端末E5および通信端末F6はそれぞれ第2実施形態における通信端末Sおよび通信端末Mにある。

【0147】ステップS312において、自機プロトコル情報ファイル323Fの「プロトコルセット」フィールドと他機プロトコル情報ファイル324Fの「プロトコルセット」フィールドの両方に同じプロトコルセットの名称を示す情報が存在し、判定結果として「Yes」を得た場合、制御部31Fは自機プロトコル情報ファイル323Fの全てのレコードの中から、「プロトコルセット」フィールドの値が他機プロトコル情報ファイル324Fの「プロトコルセット」フィールドの値のいずれかと一致するものを抽出する。この場合、複数のレコードが抽出されてもよい。続いて、制御部31Fは決定プロトコル情報ファイル325Fを読み出し、その各レコードの「自機MACアドレス」フィールドの値および「プロトコルセット」フィールドの値を、抽出された各レコードの「MACアドレス」フィールドの値（以下、「MAC-List-F」と呼ぶ）および「プロトコルセット」フィールドの値（以下、「決定プロトコルセット・リスト3」と呼ぶ）でそれぞれ更新する。続いて制御部31Fは決定プロトコル情報ファイル325Fの「他機MACアドレス」フィールドの値を更新するために、決定プロトコル情報ファイル325Fの各レコードに関して以下の動作を行う。まず制御部31Fは他機プロトコル情報ファイル324Fの全レコードの中から、その「プロトコルセット」フィールドの値が対象のレコードの「プロトコルセット」フィールドの値と一致するレコードを検索する。次に、制御部31Fは決定プロトコル情報ファイル325Fの対象のレコードの「他機MACアドレス」フィールドの値を、検索されたレコードの「MACアドレス」フィールドの値で更新する（ステップS315）。

【0148】次に、制御部31Fは決定プロトコル情報ファイル325Fを読み出し、全レコードに関し次の動作を行う。制御部31Fは自機プロトコル情報ファイル

323Fを読み出し、その全レコードの中から、その「プロトコルセット」フィールドの値が、決定プロトコル情報ファイル325Fの対象のレコードの「プロトコルセット」フィールドの値と一致するレコードを検索する。次に、制御部31Fは検索されたレコードの「パラメータセット」フィールドの値に基づいて、通信端末E5が他の通信端末と対象のレコードの「プロトコルセット」フィールドの値が示すプロトコルセットを用いて無線通信を行うために変更の必要な通信パラメータを決定する。次に、制御部31Fは決定プロトコル情報ファイル325Fの対象のレコードの「パラメータセット」フィールドの値を、決定した通信パラメータで更新する（ステップS316）。以下、ステップS316において決定された通信端末E5用の複数の通信パラメータセットを「パラメータセット・リストE」と呼ぶ。

【0149】ステップS316におけるパラメータセットの決定動作について、例を挙げて説明する。今、決定プロトコルセット・リスト3が「IEEE802.11b - TCP/IP」と「Bluetooth - NetBEUI」の2つの値を持ち、自機プロトコル情報ファイル323Fの「プロトコルセット」フィールドの値が「IEEE802.11b - TCP/IP」および「Bluetooth - NetBEUI」であるレコードの「パラメータセット」フィールドの値がそれぞれ以下の通りであったとする。

「IEEE802.11b - TCP/IP」

パラメータ1 「IEEE802.11b: モード=Ad Hoc」

パラメータ2 「IEEE802.11b: チャンネルID=3」

パラメータ3 「IPアドレス / サブネットマスク=192.168.0.220 / 255.255.255.0」

「Bluetooth - NetBEUI」

パラメータ1 「Bluetooth: PIN Code=4E63」

この場合、制御部31Fはパラメータセット・リストEとして、

「IEEE802.11b - TCP/IP」

パラメータ1 「IEEE802.11b: モード=Ad Hoc」

パラメータ2 「IEEE802.11b: チャンネルID=3」

パラメータ3 「IPアドレス / サブネットマスク=192.168.0.222 / 255.255.255.0」

「Bluetooth - NetBEUI」

パラメータ1 「Bluetooth: PIN Code=4E63」

を決定する。ここで、PIN CodeはBluetoothにおいて規定されている接続認証用のPersonal Identification Number Codeのことである。

【0150】まず、通信端末F6の属する無線通信網においては、IEEE802.11bがTCP/IPとの組み合わせで用いられている。この無線通信網においては、まずIEEE802.11bに関して、通信モードとしてAd Hocモード、チャンネルIDとして3が用いられている。これらのパラメータはこの無線通信網に参加する通信機器において同じである必要があるので、制御部31Fはパラメータセット・

リストEにこれらのコピーを追加している。またTCP/IPに関して、この無線通信網においては、IPアドレスとして192.168.0.xxx (xxxは255以下の正の整数)、サブネットマスクとして255.255.255.0が用いられている。制御部31Fは通信端末F6のIPアドレスに隣接するIPアドレスが既に使用されていないかを無線通信網にブロードキャストすることにより確認し、通信端末E5用の未使用のIPアドレス／サブネットマスクとして192.168.0.222 / 255.255.255.0をパラメータセット・リストEに追加している。また、この無線通信網においては、BluetoothがNetBEUIとの組み合わせで用いられている。Bluetoothにおいては同じ通信網内の全ての通信機器が同じPIN Codeを用いる必要があるので、制御部31Fはこれをパラメータセット・リストEに追加している。NetBEUIに関しては、この例においては設定変更を必要としていないので、制御部31Fはプロトコルセット・リストEに何も追加していない。

【0151】ステップS316においてパラメータセット・リストEを決定した後、制御部31Fは決定プロトコル情報ファイル325Fを読み出し、全レコードの「自機MACアドレス」フィールドの値、すなわちMAC-List-F、「プロトコルセット」フィールドの値、すなわち決定プロトコルセット・リスト3、「パラメータセット」フィールドの値、すなわちパラメータセット・リストEを通信端末E5に送信する（ステップS317）。これらの情報は通信端末E5が無線通信部28Eを用いて他の通信端末と通信を行うための通信パラメータである。

【0152】制御部31EはMAC-List-F、決定プロトコルセット・リスト3およびパラメータセット・リストEを通信端末F6から受信すると、決定プロトコル情報ファイル325Eを読み出し、「他機MACアドレス」フィールドの値、「プロトコルセット」フィールドの値および「パラメータセット」フィールドの値をそれぞれMAC-List-F、決定プロトコルセット・リスト3およびパラメータセット・リストEで更新する（ステップS318）。

【0153】続いて、制御部31Eは決定プロトコル情報ファイル325Eの全レコードの「プロトコルセット」フィールドの値および「パラメータセット」フィールドの値を無線通信部28Eに送信する。無線通信部28Eはこれらの情報を受信すると、不揮発性メモリに記憶されている、「プロトコルセット」フィールドの値が示す通信プロトコルセットに関する通信パラメータを、「パラメータセット」フィールドの値が示す情報に基づいて変更する。なお、この変更を終えた無線通信部28Eは、設定終了を制御部31Eに通知する（ステップS319）。

【0154】設定終了の通知を無線通信部28Eより受信すると、制御部31Eは設定完了通知を通信端末F6

に送信し（ステップS320）、通信端末F6の制御部31Fは設定完了通知を通信端末E5から受信する（ステップS321）。ステップS320を終えた後、制御部31Eは無線通信の設定が完了したことを通知するメッセージを表示部30Eに表示する（ステップS322）。同様に、ステップS321を終えた後、制御部31Fは無線通信の設定が完了したことを通知するメッセージを表示部30Fに表示する（ステップS323）。

【0155】ステップS322およびステップS323において表示されたメッセージにより、パラメータ設定が完了したことを確認した通信端末E5および通信端末F6のユーザは、有線通信部27Eと有線通信部27Fに接続していたケーブルを取り外すことができる。その後、通信端末E5は決定プロトコルセット・リスト3に含まれるプロトコルセットによって他の通信端末と無線通信が可能となる。例えば、通信端末F6が通信端末G7とはIEEE802.11b - TCP/IPにて、通信端末H8とはBluetooth - NetBEUIにて無線通信を行っているとする。この場合、通信端末E5は通信端末F6とはIEEE802.11b - TCP/IPおよびBluetooth - NetBEUIにて、通信端末G7とはIEEE802.11b - TCP/IPにて、通信端末H8とはBluetooth - NetBEUIにて無線通信が可能となる。

【0156】【3. 2. 3】公開鍵を用いた通信方法上記の通信パラメータ設定を終了した後、通信端末E5は無線通信システム3において他の通信端末と無線通信を行う際、公開鍵および秘密鍵を用いて交換される情報を暗号化および復号化する。以下、図29および図30を用いてその通信動作を説明する。なお、以下の動作は無線通信システム3において、通信端末E5と他の通信端末のいずれかとの間において行われる動作であり、その動作はどの通信端末を相手とする場合であっても同じである。従って、ここでは例として通信端末G7相手の場合を説明する。なお、通信端末E5と通信端末G7の立場が逆転しても構わない。また、以下の通信動作においては、通信端末E5と通信端末G7の間で行われる情報の送受信は全て無線通信部28Eおよび無線通信部34Gを介して行われる。今、通信端末E5が通信端末G7にある処理を要求する場合を考える。まず、通信端末E5の制御部31Eは識別子情報ファイル326Eを読み出し、通信先である通信端末G7のMACアドレス（以下、「MAC-G」と呼ぶ）が、識別子情報ファイル326Eのいずれかのレコードの「MACアドレス」フィールドの値と一致するか否かを判定する（ステップS324）。MAC-Gが識別子情報ファイル326Eのいずれかのレコードの「MACアドレス」フィールドの値と一致する場合、制御部31EはステップS324の判定結果として「Yes」を得る。MAC-Gが識別子情報ファイル326Eのいずれのレコードの「MACアドレス」フィールドの値とも一致しない場合、制御部31EはステップS324の判定結果として「No」を得る。

【0157】ステップS324で「Yes」を得た場合、制御部31Eは制御を後述するステップS329に移す。

【0158】ステップS324で「No」を得た場合、制御部31Eは通信端末G7に対し識別子要求を送信し（ステップS325）、制御部37Gは通信端末E5から識別子要求を受信する（ステップS326）。

【0159】制御部37Gは設定管理情報ファイル381Gを読み出し、「自機識別子」アイテムの値（以下、「ID-G」と呼ぶ）を通信端末E5に送信する（ステップS327）。制御部31Eは通信端末G7からID-Gを受信すると、識別子情報ファイル326Eを読み出し、新たなレコードを追加し、その追加されたレコードの「MACアドレス」フィールドの値および「識別子」フィールドの値を、それぞれMAC-GおよびID-Gとする（ステップS328）。

【0160】統いて、制御部31Eは公開鍵情報ファイル327Eを読み出し、ID-Gがいずれかのレコードの「識別子」フィールドの値と一致するか否かを判定する（ステップS329）。ID-Gが公開鍵情報ファイル327Eのいずれかのレコードの「識別子」フィールドの値と一致する場合、制御部31EはステップS329の判定結果として「Yes」を得る。ID-Gが公開鍵情報ファイル327Eのいずれのレコードの「識別子」フィールドの値とも一致しない場合、制御部31EはステップS329の判定結果として「No」を得る。

【0161】ステップS329で「Yes」を得た場合、制御部31Eは制御を後述するステップS334に移す。

【0162】ステップS329で「No」を得た場合、制御部31Eは通信端末G7に対し公開鍵要求を送信し（ステップS330）、制御部37Gは通信端末E5から公開鍵要求を受信する（ステップS331）。

【0163】制御部37Gは設定管理情報ファイル381Gを読み出し、「公開鍵」アイテムの値（以下、「Key-G」と呼ぶ）を通信端末E5に送信する（ステップS332）。制御部31Eは通信端末G7からKey-Gを受信すると、公開鍵情報ファイル327Eを読み出し、新たなレコードを追加し、追加されたレコードの「識別子」フィールドの値および「公開鍵」フィールドの値をそれぞれID-GおよびKey-Gとする（ステップS333）。ステップS333を終えた制御部31Eは制御をステップS334に移す。なお、上記ステップS324からステップS333までの動作を以下、「公開鍵取得作業1」と呼ぶ。

【0164】公開鍵更新作業1を終えた後、制御部31Eは通信端末G7に対する処理要求情報を準備する。この処理要求情報は通信端末G7に対する処理の要求に加え、処理に必要なデータを含んでいる（ステップS334）。次に、制御部31Eは準備した処理要求情報をKe

y-Gを用いて暗号化し、暗号化した処理要求情報を通信端末G7に送信する（ステップS335）。

【0165】通信端末G7の制御部37Gは暗号化された処理要求情報を受信すると、設定管理情報ファイル321Fを読み出し、「秘密鍵」アイテムの値を用いて暗号化された処理要求情報を復号化する（ステップS336）。

【0166】制御部37Gは復号化された処理要求情報に従って処理を行い、その処理結果情報を作業領域384Gに保存する（ステップS337）。

【0167】ステップS337を終えた後、通信端末E5および通信端末G7は上述した公開鍵取得作業1（ステップS324からステップS333まで）の動作と同様の動作として、公開鍵取得作業2を行う（ステップS338からステップS347）。この公開鍵取得作業2は通信端末E5と通信端末G7の立場を入れ替えただけのものであるので、説明は省略する。

【0168】公開鍵更新作業2を終えた後、制御部37Gは作業領域384GからステップS337において保存した処理結果情報を読み出す。また、制御部37Gは公開鍵情報ファイル383Gを読み出し、「識別子」フィールドの値が通信端末E5の識別子（以下、「MAC-E」と呼ぶ）と一致するレコードを検索し、検索されたレコードの「公開鍵」フィールドの値（以下、「Key-E」と呼ぶ）を取り出す。制御部37Gは処理結果情報をKey-Eを用いて暗号化した後、通信端末E5に送信する（ステップS348）。

【0169】通信端末E5の制御部31Eは、暗号化された処理結果情報を受信すると、設定管理情報ファイル321Eを読み出し、「秘密鍵」アイテムの値を用いて暗号化された処理結果情報を復号化する（ステップS349）。こうして、制御部31Eは通信端末G7に要求した処理結果を受信する。

【0170】[3. 3] 第3実施形態の効果

第3実施形態においては、新たに無線通信網に加わる通信端末のユーザが自分の通信端末を既に無線通信網に接続している通信端末とケーブルにて接続する、という直感的に理解可能な方法によって無線通信のパラメータ設定を行うことができ、その他、アプリケーションソフトを起動する等の手間を要しない。これはユーザにとっての通信パラメータ設定準備作業を大幅に軽減する。

【0171】第3実施形態において、通信パラメータ設定時に新たに無線通信網に加わる通信端末のユーザが行うべきことは、ユーザが自分で任意に登録したパスワードの入力のみである。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。なお、この通信パラメータ設定においては、利用可能な通信プロトコルが複数選ばれるため、アクセスポイントによる無線通信の中継を介さずとも、無線通信網の多くの通信端末との通信が可能となる。

【0172】第3実施形態において実現される無線通信システム3においては、通信端末間の情報は全て暗号化されるため、部外者の通信機器がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。多くの無線通信プロトコルは暗号化の方法を有しているが、必ずしも暗号化は義務づけられていない。新たに無線通信網に接続する通信端末のユーザはその無線通信網において暗号化が用いられているか否かを知ることは困難であり、また暗号化がなされていないと分かっても、既に稼働している無線通信網の設定を変更することは容易ではない。これに対し本発明の第3実施形態における通信パラメータ設定によれば、既存の無線通信網に変更を加えることなく、暗号化の使用を確実に行うことことができる。

【0173】[4] 第4実施形態

[4. 1] 第4実施形態の構成

[4. 1. 1] 無線通信システムの構成

本発明の第4実施形態においては、本発明の通信パラメータ設定方法により、無線通信を中継するアクセスポイントを介して既に複数の無線通信機器が通信を行っている無線通信網に対し新たに通信機器が無線接続し、この新たに参加する通信機器が前記アクセスポイントに接続している全ての通信機器と無線を介した通信を行うことが可能となる。図31に本発明の第4実施形態における通信パラメータ設定段階の状態と通信パラメータ設定後の状態を示す。本発明の第4実施形態により実現される通信パラメータ設定後の無線通信システムを以下、「無線通信システム4」と呼ぶ。

【0174】第4実施形態においては、まず無線通信を中継するアクセスポイント10があり、このアクセスポイント10は無線通信により通信端末J11と接続されている。また、アクセスポイント10は有線通信により通信端末K12およびネットワークサーバ13と接続されている。また、アクセスポイント10は有線通信により接続されているインターネットを介して、遠距離にある本社データベースに接続が可能である。なお、有線通信および無線通信によって、アクセスポイント10はプリンター(図示略)やスキャナー(図示略)等の周辺機器とも接続されている。

【0175】この既に機能している通信網において、まだ未接続の通信端末I9をアクセスポイント10に赤外線で接続することにより、通信端末I9に対して本発明による通信パラメータ設定が行われる。その結果、通信端末I9はアクセスポイント10を介して通信端末J11、通信端末K12、インターネット、プリンターやスキャナー等の周辺機器との通信を行うことが可能となる。

【0176】第4実施形態においては、通信端末I9が無線通信システム4における通信を行うための通信パラメータの決定を要求する側の通信機器、アクセスポイント10が通信パラメータの決定を行う側の通信機器となる。アクセスポイント10は通信端末I9が無線通信システム4における無線通信を行うための通信パラメータを決定し、その決定された通信パラメータを通信端末I9に送信する。通信端末I9はアクセスポイント10から通信パラメータを受信し、自分の通信機器に対しその情報に従ったパラメータの変更を行う。この際、第4実施形態においては第2実施形態および第3実施形態と同様に、TCP/IP等の中位レイヤに関する通信プロトコルのパラメータ設定も併せて行う。

【0177】ここでは説明例として、この第4実施形態における通信網はA社B支部Cセクションのものとする。A社の本社データベースは、A社の全ての通信機器の識別子をその属するセクション名とともに記憶しており、これらの情報は常に新しいものに更新されている。

【0178】A社の本部および全ての支部の通信網においては、共有フォルダ、共有プリンター等のネットワーク資源のそれぞれは、それぞれのアカウント・グループに対し一定のアクセス権限を設定しており、ネットワークサーバ13がこれらのアクセス権限を管理している。アカウント・グループには、「同支部同セクション」

「同支部他セクション」「他支部」がある。アクセス権限には、読み取り、変更、削除を許可する「フルアクセス」、読み取りのみを許可する「読み取り専用」、利用を禁止する「アクセス拒否」がある。例えばある共有フォルダは同支部同セクションに属するユーザ・アカウントに対してはフルアクセス、同支部他セクションに属するユーザ・アカウントに対しては読み取り専用、他支部に属するユーザ・アカウントに対してはアクセス拒否のようにアクセス権限を設定している。

【0179】アクセスポイント10は有線通信によりネットワークサーバ13と接続しているが、アクセスポイント10は第4実施形態における通信網に対し、3つの異なるユーザ・アカウントによって同時にログインしている。1つは同支部同セクションに属するユーザ・アカウント(以下このユーザ・アカウントを「アカウントP1」と呼ぶ)、1つは同支部他セクションに属するユーザ・アカウント(以下このユーザ・アカウントを「アカウントP2」と呼ぶ)、他の1つは他支部に属するユーザ・アカウント(以下このユーザ・アカウントを「アカウントP3」と呼ぶ)である。

【0180】[4. 1. 2] 通信機器の構成

[4. 1. 2. 1] 新規参入する通信端末の構成

図32に、第4実施形態において新たにアクセスポイントを介して通信網へ接続を行う通信端末I9の構成を示す。

【0181】通信端末I9は赤外線通信部40、無線通信部41、操作部42、表示部43、制御部44および記憶部45を備えている。これらの構成要素はバス46を介して電気的に接続されている。

【0182】無線通信部41、操作部42、表示部43、制御部44の機能および構成は第2実施形態における通信端末C3の無線通信部21、操作部22、表示部23、制御部24のものと同様であるので、説明を省略する。また、記憶部45の機能も第2実施形態における通信端末C3の記憶部25のものと同様であるので、説明を省略する。

【0183】赤外線通信部40は他の通信機器の赤外線通信部と赤外線により接続され、通信端末I9が他の通信機器と無線通信を行う為に必要な通信パラメータ等の情報を送受信する。赤外線通信部40はアンテナ(図示略)を有し、このアンテナを介して変調された信号を受信すると、この受信した信号をベースバンド信号に復調し、ベースバンド信号を制御部44に送信する。また、赤外線通信部40は制御部44よりベースバンド信号を受け取ると、これを用いてキャリアを変調し、変調した信号を前記アンテナを介して外部に送信する。赤外線通信部40と同種の通信部を持つ全ての通信機器は共通した赤外線用通信プロトコルを1つ共有しており、通信端末I9はその赤外線用通信プロトコルを用いて、これらの赤外線通信部を介した情報の送受信を行う。

【0184】記憶部45は、設定管理情報ファイル451、自機プロトコル情報ファイル452、他機プロトコル情報ファイル453および決定プロトコル情報ファイル454を記憶し、また作業領域455を有している。

【0185】自機プロトコル情報ファイル452、他機プロトコル情報ファイル453、決定プロトコル情報ファイル454および作業領域455の構成に関しては第2実施形態における通信端末C3の自機プロトコル情報ファイル253、他機プロトコル情報ファイル254、決定プロトコル情報ファイル255および作業領域256のものと同様であるので、説明を省略する。

【0186】図33は設定管理情報ファイル451の構成を例示したものである。設定管理情報ファイル451は、「自機識別子」アイテム、「パスワード」アイテム、「秘密鍵」アイテム、「公開鍵」アイテム、「共通鍵」アイテムを持つ。「自機識別子」アイテムおよび

「パスワード」アイテムの機能は第2実施形態における通信端末C3の設定管理情報ファイル251のものと同様である。「秘密鍵」アイテムは、無線通信パラメータの設定段階において通信端末I9がアクセスポイント10から暗号化された通信情報を受信する際、その通信情報を復号化するための暗号鍵情報を含む。「公開鍵」アイテムは、無線通信パラメータの設定段階においてアクセスポイント10が通信端末I9に対し情報を送信する際、その通信情報を暗号化するための暗号鍵情報を含む。「秘密鍵」アイテムの値と「公開鍵」アイテムの値は1対をなし、「公開鍵」アイテムの値によって暗号化された情報は「秘密鍵」アイテムの値によってのみ、復号化される。「共通鍵」アイテムは無線通信システム4

において通信端末I9がアクセスポイント10を介して他の通信機器と通信を行う際、送受信される情報を暗号化および復号化する為の暗号鍵情報を含む。

【0187】[4. 1. 2. 2] アクセスポイントの構成

図34を用いて、第4実施形態において無線通信を中継するアクセスポイント10の構成を説明する。

【0188】アクセスポイント10は赤外線通信部47、無線通信部48、有線通信部49、制御部50および記憶部51を備えている。これらの構成要素はバス52を介して電気的に接続されている。

【0189】赤外線通信部47の機能および構成は通信端末I9の赤外線通信部40のものと同様であるので、説明を省略する。また無線通信部48の機能および構成は第2実施形態における通信端末C3の無線通信部21のものと同様であるので、説明を省略する。また、記憶部51の機能も第2実施形態における通信端末C3の記憶部25のものと同様であるので、説明を省略する。

【0190】有線通信部49は他の通信機器の有線通信部とLANケーブルや光ケーブル等にて接続され、アクセスポイント10が他の通信機器と有線通信を行う際の情報の送受信を行う。有線通信部49は外部より電気信号もしくは光信号を受け取ると、これを制御部50が判読可能な電気信号に変換した後に転送する。また制御部50より電気信号を受け取ると、これを外部の通信機器が判読可能な電気信号もしくは光信号に変換した後に転送する。

【0191】制御部50の構成は第2実施形態の通信端末C3における制御部24と同様であるが、無線通信部48を経由して送受信される情報量の履歴を作業領域518に記録し、その履歴を用いて定期的に各通信プロトコルセットの処理速度を推定し、推定された処理速度が速いものから優先順位を振り直す機能を有する。この優先順位が変わると、制御部50は記憶部から後述する自機プロトコル情報ファイル513を読み出し、「優先順位」フィールドの値を変化後の優先順位を示す正の整数值で更新する。

【0192】記憶部51は、設定管理情報ファイル511、アクセストラップ情報ファイル512、自機プロトコル情報ファイル513、他機プロトコル情報ファイル514、決定プロトコル情報ファイル515、識別子情報ファイル516および共通鍵情報ファイル517を記憶し、また作業領域518を有している。

【0193】自機プロトコル情報ファイル513、他機プロトコル情報ファイル514、決定プロトコル情報ファイル515および作業領域518の構成に関しては第2実施形態における通信端末C3の自機プロトコル情報ファイル253、他機プロトコル情報ファイル254、決定プロトコル情報ファイル255および作業領域256のものと同様であるので、説明を省略する。識別子情

報ファイル516の構成に関しては、第3実施形態における通信端末E5の識別子情報ファイル326のものと同様であるので、説明を省略する。

【0194】図35は設定管理情報ファイル511の構成を例示したものである。設定管理情報ファイル511は「他機識別子」アイテムおよび「他機公開鍵」アイテムを持つ。「他機識別子」アイテムは新規にアクセスポイント10を介して通信網に接続を行う通信端末の識別子を含む。「他機公開鍵」アイテムは、アクセスポイント10が新規にこのアクセスポイントを介して通信網に接続を行う通信端末に対し、通信パラメータ設定段階における情報を送信する際に、その情報を暗号化する為の暗号鍵情報を含む。

【0195】図36はアクセス権限情報ファイル512の構成を例示したものである。アクセス権限情報ファイル512はA社の本社データベースに登録されている通信機器の数と等しい数のレコードを持ち、各レコードは1つの通信機器に関する情報の集まりである。各レコードには「識別子」フィールドと「アカウント・グループ」フィールドがあり、「識別子」フィールドは通信機器の識別子を、「アカウント・グループ」フィールドはアクセスポイント10が属するA社B支部Cセクションにおいて、対象の通信機器が属するアカウント・グループの情報を含む。アクセスポイント10は定期的にインターネットを介して本社データベースから登録されている通信機器の識別子および所属のセクション名をダウンロードする。その際、アクセスポイント10は所属のセクション名を1つづつ読み出し、その値がA社B支部Cセクションを示すものであれば「同支部同セクション」、A社B支部であるがCセクション以外のセクションを示すものであれば「同支部他セクション」、A社の他支部を示すものであれば、「他支部」に変換する。そして、「識別子」フィールドの値をダウンロードした識別子で、また「アカウント・グループ」フィールドの値を変換した後の、各通信機器のアカウント・グループを示す情報で更新する。

【0196】図37は共通鍵情報ファイル517の構成を例示したものである。共通鍵情報ファイル517は今までにアクセスポイント10に接続した通信機器の数と等しい数のレコードを持つ。各レコードは「識別子」フィールドと「共通鍵」フィールドを持つ。「識別子」フィールドは対象の通信機器の識別子を含み、「共通鍵」フィールドはアクセスポイント10が対象の通信機器と無線通信部48もしくは有線通信部49を介した通信を行う際、通信する情報を暗号化および復号化する為の暗号鍵情報を含む。

【0197】アクセスポイント10は操作部および表示部を持たないが、管理者は赤外線通信部47、無線通信部48もしくは有線通信部49を介し、他の通信機器より操作を行うことができる。

【0198】[4. 1. 2. 3] 新規参入する通信端末以外の通信端末の構成

第4実施形態において、新たに通信網に接続する通信端末以外の通信端末は同じ構成であるので、図38を用いて通信端末J11の構成を説明し、通信端末K12の説明は省略する。

【0199】通信端末J11は通信部53、操作部54、表示部55、制御部56および記憶部57を備えている。これらの構成要素はバス58を介して電気的に接続されている。

【0200】操作部54、表示部55および制御部56の機能および構成は第2実施形態における通信端末C3の操作部22、表示部23および制御部24のものと同様であるので、説明を省略する。また、記憶部57の機能も第2実施形態の通信端末C3における記憶部25のものと同様であるので、説明を省略する。

【0201】通信部53は他の通信機器の通信部と有線もしくは無線により接続され、通信端末J11が他の通信機器と通信を行う際の情報の送受信を行う。通信部53は外部より電気信号、光信号、もしくは電波信号を受け取ると、これを制御部56が判読できる電気信号に変換後、これを制御部56に転送する。また、制御部56より電気信号を受け取ると、これを他の通信機器が判読可能な電気信号もしくは電磁波信号に変換した後に転送する。

【0202】記憶部57は、設定管理情報ファイル571を記憶し、また作業領域572を有している。

【0203】作業領域572の機能に関しては第2実施形態における通信端末C3の作業領域256のものと同様であるので、説明を省略する。

【0204】図39は設定管理情報ファイル571の構成を例示したものである。設定管理情報ファイル571は「自機識別子」アイテムおよび「共通鍵」アイテムを持つ。「自機識別子」アイテムの機能は第2実施形態における通信端末C3の設定管理情報ファイル251のものと同様である。また、「共通鍵」アイテムは通信端末J11がアクセスポイント10と通信部53を介して通信する際、情報を暗号化および復号化する為の暗号鍵情報を含む。

【0205】[4. 2] 第4実施形態の動作

第4実施形態において、無線通信システム4を実現するための通信パラメータ設定および通信パラメータ設定後の通信方法の動作例を説明する。以下の説明において、通信端末I9とアクセスポイント10の同種の構成要素を区別するために、各構成要素を特定する符号に“I”および“P”を付加する。

【0206】[4. 2. 1] 接続認証及びパラメータ設定段階

はじめに、アクセスポイント10は通信端末I9がアクセスポイント10に接続することの認証作業を行う。続

いてアクセスポイント10は通信端末I9が無線通信のために必要とする通信パラメータの決定を行い、通信端末I9はアクセスポイント10により決定された通信パラメータに従い、通信パラメータの変更を行う。以下、図40および図41を用いてその動作説明を行う。なお、以下の接続認証およびパラメータ設定段階においては、通信端末I9とアクセスポイント10の間で行われる情報の送受信は全て赤外線通信部401および赤外線通信部47Pを介して行われる。

【0207】まず、通信端末I9のユーザはアクセスポイント10の赤外線通信部47Pを見通せる位置に通信端末I9を置く。赤外線通信部401および赤外線通信部47Pは相手から送信される赤外線信号を検知し、赤外線接続を確立する（ステップS401）。

【0208】制御部44Iは次にパスワード照合作業を行う。このパスワード照合作業は第2実施形態におけるステップS206からS08と同様であるので、説明を省略する（ステップS402からステップS404）。なお、このパスワード入力作業は、正しいユーザが通信端末I9の無線通信網に対する接続を試みていることを確認するための動作である。

【0209】ステップS404において2つのパスワードが一致した場合、制御部44Iは秘密鍵と公開鍵のセットを新たに生成し、設定管理情報ファイル451Iを読み出し、「秘密鍵」アイテムの値および「公開鍵」アイテムの値をそれぞれ生成した秘密鍵および公開鍵の情報で更新する。ここで、秘密鍵と公開鍵の生成の方法については既に知られる方法によるので、説明を省略する（ステップS405）。

【0210】次に、制御部44Iは設定管理情報ファイル451Iおよび自機プロトコル情報ファイル452Iを読み出し、まず設定管理情報ファイル451Iの「自機識別子」アイテムの値（以下、「ID-I」と呼ぶ）および「公開鍵」アイテムの値（以下、「Key-I」と呼ぶ）を取り出す。続いて、制御部44Iは自機プロトコル情報ファイル452Iの全レコードの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値（以下、「プロトコルセット・テーブルI」と呼ぶ）を各レコードにおける対応関係を維持したままで取り出す。プロトコルセット・テーブルIは通信端末I9が無線通信部41Iを用いた通信を行う際に利用可能なプロトコルに関する案内情報である。次に、制御部44IはID-I、Key-I、およびプロトコルセット・テーブルIをアクセスポイント10に送信する（ステップS406）。アクセスポイント10の制御部50PはID-I、Key-Iおよびプロトコルセット・テーブルIを受信すると、まず設定管理情報ファイル511Pを読み出し、その「他機識別子」アイテムの値をID-Iで、「他機公開鍵」アイテムの値をKey-Iで更新する。続いて、制御部50Pは他機プロトコル情報ファイル514Pを読み出し、

その「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値をプロトコルセット・テーブルIの「MACアドレス」フィールドおよび「プロトコルセット」フィールドの値でそれぞれ更新する（ステップS407）。

【0211】続いて、制御部50Pはアクセス権限情報ファイル512Pを読み出し、ID-Iがいずれかのレコードの「識別子」フィールドの値と一致するか否かを判定する（ステップS408）。ID-Iがアクセス権限情報ファイル512Pのいずれかのレコードの「識別子」フィールドの値と一致する場合、制御部50PはステップS408の判定結果として「Yes」を得る。ID-Iがアクセス権限情報ファイル512Pのいずれのレコードの「識別子」フィールドの値とも一致しない場合、制御部50PはステップS408の判定結果として「No」を得る。

【0212】ステップS408で「Yes」を得ると、制御部50Pは制御を後述するステップS411に移す。

【0213】ステップS408で「No」を得ると、制御部50Pは接続拒絶通知を通信端末I9に送信する（ステップS409）。これは、通信端末I9が登録されておらず、この無線通信網への接続が拒否されたことを意味する。通信端末I9の制御部44Iはアクセスポイント10より接続拒絶通知を受信すると、接続が拒絶されたことを通知するメッセージを表示部43Iに表示する（ステップS410）。このステップを経た場合、制御部44Iは動作を終了する。

【0214】ステップS408において制御部50Pが「Yes」の判定を得た場合、通信端末I9およびアクセスポイント10は通信可能確認作業を行う。通信可能確認作業は第2実施形態におけるステップS220からS22とほぼ同様であるので、詳細な説明を省略する（ステップS411からステップS413）。この通信可能確認作業において、通信端末I9およびアクセスポイント10はそれぞれ第2実施形態における通信端末Sおよび通信端末Mにあたる。ただし、ステップS412において、制御部50Pは無線通信の設定が不可能であることを通知するメッセージの表示を行わない。

【0215】ステップS411の判定結果として「Yes」を得た場合、制御部50Pは自機プロトコル情報ファイル513Pを読み出し、その全てのレコードの中から、「プロトコルセット」フィールドの値が他機プロトコル情報ファイル514Pのいずれかのレコードの「プロトコルセット」フィールドの値と一致するレコードを全て抽出する。自機プロトコル情報ファイル513Pから複数のレコードが抽出された場合、制御部50Pは抽出されたレコードの「優先順位」フィールドの値を比較し、「優先順位」フィールドの値が最も小さいものを選択する。一つのレコードのみが抽出された場合、制御部

50Pはそのレコードを選択する。次に、制御部50Pは決定プロトコル情報ファイル515Pを読み出し、その唯一のレコードの「自機MACアドレス」フィールドの値を選択されたレコードの「MACアドレス」フィールドの値（以下、「MAC-P」と呼ぶ）で、「プロトコルセット」フィールドの値を選択されたレコードの「プロトコルセット」フィールドの値（以下、「決定プロトコルセット4」と呼ぶ）で更新する。続いて、制御部50Pは他機プロトコル情報ファイル514Pの全てのレコードの中から、「プロトコルセット」フィールドの値が決定プロトコルセット4と一致するレコードを検索し、決定プロトコル情報ファイル515Pの「他機MACアドレス」フィールドの値を検索されたレコードの「MACアドレス」フィールドの値（以下、「MAC-I」と呼ぶ）で更新する（ステップS414）。

【0216】次に、制御部50PはステップS414において選択された自機プロトコル情報ファイル513Pのレコードの「パラメータセット」フィールドの値に基づいて、通信端末I9がアクセスポイント10と決定プロトコルセット4の示すプロトコルセットを用いて無線通信を行うために変更の必要なパラメータセットの値を決定する。以下、通信端末I9用のパラメータセットを「パラメータセットI」と呼ぶ。次に制御部50Pは決定プロトコル情報ファイル515Pを読み出し、その唯一のレコードの「パラメータセット」フィールドの値をパラメータセットIで更新する（ステップS415）。なお、パラメータセットの決定方法は第2実施形態および第3実施形態におけるパラメータセットの決定方法と同様であるので、説明を省略する。

【0217】次に、制御部50Pは通信端末I9がアクセスポイント10と無線通信部41Iと無線通信部48Pを用いて通信を行う際に通信情報を暗号化および復号化する任意の暗号鍵（以下、「Key'-I」と呼ぶ）を作成する。暗号鍵は文字、数字および記号の列であり、乱数関数により生成される。乱数関数については既に多くの既知のものがあるため、ここでは説明を省略する。続いて、制御部50Pは設定管理情報ファイル511Pを読み出し、「他機識別子」アイテムの値、すなわちID-Iを取り出す。次に共通鍵情報ファイル517Pを読み出し、「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値をKey'-Iで更新する。共通鍵情報ファイル517Pのいずれのレコードの「識別子」フィールドの値もID-Iと一致しない場合には、制御部50Pは共通鍵情報ファイル517Pに新たなレコードを追加し、追加されたレコードの「識別子」フィールドの値をID-Iとし、「共通鍵」フィールドの値をKey'-Iとする（ステップS416）。

【0218】続いて、制御部50Pは設定管理情報ファイル511Pを読み出し、「他機識別子」アイテムの

値、すなわちID-Iと、「他機公開鍵」アイテムの値、すなわちKey-Iを取り出す。次に制御部50Pは共通鍵情報ファイル517Pを読み出し、「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Iを取り出す。次に、制御部50Pは決定プロトコル情報ファイル515Pを読み出し、唯一のレコードの「自機MACアドレス」フィールドの値、すなわちMAC-P、「プロトコルセット」フィールドの値、すなわち決定プロトコルセット4、「パラメータセット」フィールドの値、すなわちパラメータセットI、を取り出す。これらの情報は通信端末I9が無線通信部41Iを用いてアクセスポイント10と通信を行うための通信パラメータである。続いて、制御部50PはMAC-P、決定プロトコルセット4、パラメータセットIおよびKey'-Iを用いて暗号化した後、それらを通信端末I9に送信する（ステップS417）。

【0219】通信端末I9の制御部44IはMAC-P、決定プロトコルセット4、パラメータセットIおよびKey'-Iを含む暗号化された情報を受信すると、設定管理情報ファイル451Iを読み出し、受信した情報を「秘密鍵」アイテムの値で復号化する。続いて、制御部44Iは決定プロトコル情報ファイル454Iを読み出し、唯一のレコードの「他機MACアドレス」フィールドの値、「プロトコルセット」フィールドの値、「パラメータセット」フィールドの値をそれぞれMAC-P、決定プロトコルセット4、パラメータセットIで更新する。次に、制御部44Iは自機プロトコル情報ファイル452Iを読み出し、「プロトコルセット」フィールドの値が決定プロトコルセット4と一致するレコードを検索する。続いて、制御部44Iは決定プロトコル情報ファイル454Iの唯一のレコードの「自機MACアドレス」フィールドの値を、検索されたレコードの「MACアドレス」フィールドの値、すなわちMAC-Iで更新する。次に、制御部44Iは設定管理情報ファイル451Iを読み出し、「共通鍵」アイテムの値をKey'-Iで更新する（ステップS418）。

【0220】制御部44Iは決定プロトコル情報ファイル454Iを読み出し、唯一のレコードの「プロトコルセット」フィールドの値および「パラメータセット」の値を無線通信部41Iに送信する。無線通信部41Iはこれらの情報を受信すると、不揮発性メモリに記憶されている、「プロトコルセット」フィールドの値が示す通信プロトコルセットに関する通信パラメータを、「パラメータセット」フィールドの値が示す情報に基づいて変更する。なお、この変更を終えた無線通信部41Iは、設定終了を制御部44Iに通知する（ステップS419）。

【0221】設定終了の通知を無線通信部41Iより受信すると、制御部44Iは無線通信の設定が完了したこ

とを通知するメッセージを表示部43Iに表示する（ステップS420）。

【0222】ステップS420において表示されたメッセージにより、パラメータ設定が完了したことを確認した通信端末I9のユーザは、赤外線通信部40Iを介したアクセスポイント10との通信接続を切断することができる。その後、通信端末I9のユーザは決定プロトコルセット4の示すプロトコルセットによって、アクセスポイント10を介して他の通信端末との無線通信が可能となる。

【0223】[4.2.2] 共通鍵を用いた通信方法
上記の通信パラメータ設定を終了した後、通信端末I9が無線通信システム4において他の通信機器と通信を行う際、通信情報は共通鍵を用いて暗号化される。また、アクセスポイント10は通信端末I9が無線通信網の共有資源を利用する場合、通信端末I9の代行としてそれらにアクセスすることにより、ネットワークサーバ13が通信端末I9のアクセス権限管理を行うことを可能にする。図42および図43を用いてその動作説明を行う。なお、以下の動作は通信端末I9がアクセスポイント10を介して通信端末J11にある処理を要求する場合の例である。また、説明の為、本例においては通信端末I9はA社D支部Eセクションに属するものであるとする。以下、通信端末I9、アクセスポイント10および通信端末J11の同種の構成要素を区別するために、各構成要素を特定する符号にそれぞれ“I”、“P”および“J”を付加する。また、以下の動作においては、通信端末I9とアクセスポイント10の間で行われる情報の送受信は全て無線通信部41Iおよび無線通信部48Pを介して、アクセスポイント10と通信端末J11の間で行われる情報の送受信は全て無線通信部48Pもしくは有線通信部49Pおよび通信部53Jを介して行われる。

【0224】まず、制御部44Iは通信端末J11に対する処理要求情報を準備する（ステップS421）。この処理要求情報は通信端末J11のMACアドレス（以下、「MAC-J」と呼ぶ）、通信端末J11に対する処理の要求に加え、処理に必要なデータを含んでいる。次に、制御部44Iは設定管理情報ファイル451Iを読み出し、「共通鍵」アイテムの値、すなわちKey'-Iを取り出し、処理要求情報をKey'-Iを用いて暗号化する。次に、制御部44Iは決定プロトコル情報ファイル454Iを読み出し、唯一のフィールドの「自機MACアドレス」フィールドの値、すなわちMAC-Iを取り出し、暗号化された処理要求情報にMAC-Iを付加して、これをアクセスポイント10に送信する（ステップS422）。

【0225】アクセスポイント10の制御部50PはMAC-Iが付加された、暗号化された処理要求情報を受信すると、識別子情報ファイル516Pを読み出し、その全レコードから「MACアドレス」フィールドの値がMAC-Iと

一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値、すなわちID-Iを取り出す。次に、制御部50Pは共通鍵情報ファイル517Pを読み出し、その全レコードから「識別子」フィールドの値がID-Iと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Iを取り出す。制御部50Pは暗号化された処理要求情報をKey'-Iを用いて復号化する。制御部50Pはこの処理要求情報をKey'-Iと共に作業領域518Pに保存する（ステップS423）。

【0226】次に、制御部50Pはアクセス権限情報ファイル512Pを読み出し、その全レコードから「識別子」フィールドの値がステップS423で取り出したID-Iと一致するレコードを検索し、検索されたレコードの「アカウント・グループ」フィールドの値を取り出す（ステップS424）。ここで、第4実施形態における通信網はA社B支部Cセクションに所属し、通信端末I9はA社D支部Eセクションに所属することから、ここで検索されたレコードの「アカウント・グループ」フィールドの値は「他支部」となっている。

【0227】続いて、制御部50Pは作業領域518Pから処理要求情報を読み出し、処理要求情報からこの処理要求の宛先であるMAC-Jを取り出す。次に、制御部50Pは識別子情報ファイル516Pを読み出し、その全レコードから「MACアドレス」フィールドの値がMAC-Jと一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値（以下、「ID-J」と呼ぶ）を取り出す。次に、制御部50Pは共通鍵情報ファイル517Pを読み出し、その全レコードから「識別子」フィールドの値がID-Jと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値（以下、「Key'-J」と呼ぶ）を取り出す。制御部50Pは処理要求情報をKey'-Jを用いて暗号化する。次に、制御部50Pは暗号化された処理要求情報に対し、送信元ユーザ・アカウント情報として「アカウントP3」を付加し、通信端末J11に送信する（ステップS425）。アカウントP3は既述のとおり、アクセスポイント10が「他支部」に属するユーザとしてログインしているユーザ・アカウントであり、通信端末I9に対応するアカウント・グループが他支部であることから、制御部50PはここでアカウントP3を選択している。

【0228】通信端末J11の制御部56Jは暗号化された処理要求情報を受信すると、設定管理情報ファイル571Jを読み出し、「共通鍵」アイテムの値、すなわちKey'-Jを用いて暗号化された処理要求情報を復号化する（ステップS426）。

【0229】制御部56Jは受信した処理要求情報に基づき処理を行うが、その処理を行うに当たり通信網の共有ネットワーク資源を利用する必要が生じると、制御部56Jはネットワークサーバ13に対し、アカウントP3

に与えられている、そのネットワーク資源に関するアクセス権限情報を要求する。ネットワークサーバ13はこの要求に応じて、アカウントP3が対象のネットワーク資源に対し有しているアクセス権限情報を通信端末J11に送信する。制御部56Jは受信した情報に基づき、要求されている処理がアカウントP3に与えられているアクセス権限によって可能か否かを判定する(ステップS427)。処理に必要な動作がアカウントP3のアクセス権限では実行できない場合、制御部56JはステップS427の判定結果として「No」を得、処理を中断する。要求された処理を行うための全ての動作がアカウントP3のアクセス権限で実行できる場合、制御部56JはステップS427の判定結果として「Yes」を得る。

【0230】ステップS427において「No」を得ると、制御部56Jは処理拒絶通知をアクセスポイント10に送信する(ステップS428)。アクセスポイント10の制御部50Pは通信端末J11より処理拒絶通知を受信すると、その通知を通信端末I9に転送する(ステップS429)。通信端末I9の制御部44Iはアクセスポイント10より処理拒絶通知を受信すると、表示部43Iに処理が拒絶されたことを通知するメッセージを表示する(ステップS430)。ステップS430を終えると、制御部44Iの動作は終了する。

【0231】ステップS427において「Yes」を得ると、制御部56Jは要求された処理を完了する(ステップS431)。要求された処理が終了すると、制御部56Jは設定管理情報ファイル571Jを読み出し、を取り出し、処理結果情報を「共通鍵」アイテムの値、すなわちKey'-Jを用いて暗号化する。次に、制御部56Jは暗号化された処理結果情報に送信元のMACアドレスとしてMAC-Jを付加した後、これをアクセスポイント10に送信する(ステップS432)。

【0232】アクセスポイント10の制御部50PはMAC-Jの付加された暗号化された処理結果情報を受信すると、識別子情報ファイル516Pを読み出し、その全レコードから「MACアドレス」フィールドの値が処理結果情報に付加されているMAC-Jと一致するレコードを検索し、検索されたレコードの「識別子」フィールドの値、すなわちID-Jを取り出す。次に、制御部50Pは共通鍵情報ファイル517Pを読み出し、その全レコードから「識別子」フィールドの値がID-Jと一致するレコードを検索し、検索されたレコードの「共通鍵」フィールドの値、すなわちKey'-Jを取り出す。制御部50Pは処理結果情報をKey'-Jを用いて復号化する(ステップS433)。

【0233】次に、制御部50Pは作業領域518PからステップS423において保存した処理要求情報およびKey'-Iを読み出す。そして、制御部50Pは復号化された処理結果情報がこの処理要求情報に対するものであることを確認し、処理結果情報をKey'-Iを用いて暗号化

する。制御部50Pは暗号化された処理結果情報を通信端末I9に送信する(ステップS434)。

【0234】通信端末I9の制御部44Iは暗号化された処理結果情報を受信すると、設定管理情報ファイル451Iを読み出し、「共通鍵」フィールドの値、すなわちKey'-Iを用いて暗号化された処理結果情報を復号化する(ステップS435)。上記の動作により、制御部44Iは通信端末J11に対し要求した処理の結果を受信することができる。

10 【0235】【4. 3】第4実施形態の効果

第4実施形態においては、無線通信網に新たに参入を望む通信端末のユーザは、この無線通信網における通信の中継を行っているアクセスポイントの近くに通信端末を置き、ユーザが自分で任意に登録したパスワードの入力を行うだけでよい。それにより、自動的に無線通信のパラメータ設定が行われる。これはユーザにとっての通信パラメータ設定作業を大幅に軽減する。また、通信パラメータ設定時に用いられる赤外線接続は通信機器が互いに見通しがきく範囲内における近距離無線接続であるので、アクセスポイントが手の届きにくい場所に設置されても通信パラメータ設定が可能であると同時に、見えないところで部外者が通信機器の接続を試みることを防ぐことができる。これにより、高い利便性とセキュリティを両立できる。

【0236】第4実施形態においては、通信パラメータ設定作業において利用可能な通信プロトコルのうち、処理速度が最も速いと推定される通信プロトコルが選択されるため、効率の高い通信網が実現される。

【0237】第4実施形態におけるアクセスポイントは新たな通信端末の接続を、通信端末の所属情報により認証する。これにより、部外者の通信端末が通信網に接続することを防ぐことができる。

【0238】無線通信システム4においては、新たに参入した通信端末と他の通信機器間の情報は全て暗号化されるため、部外者の通信端末がその情報を受信した場合においても、その情報の内容の漏洩を防ぐことができる。暗号化には共通鍵が用いられ、高い通信速度を実現できる。また、それぞれの通信機器に対応した共通鍵をアクセスポイントが集中管理することにより、管理者の負担が軽減される。

【0239】無線通信システム4においては、新たに参入した通信端末の所属情報に基づき、その通信端末が通信網において行うネットワーク資源へのアクセスが管理される。その際、既存の通信網の設定には何ら変更が加えられない。これは通信網のアクセス権限管理に要する作業を大幅に軽減する。

【0240】

【発明の効果】上述したように、本発明によれば、無線通信網において新たな通信端末を接続する際、誰もが簡単に必要となるパラメータ設定を行うことが可能とな

る。その際、ユーザや管理者の介入なく、適当な通信プロトコルが選択される。さらに、本発明によれば、新たな通信端末が無線通信網に接続した後、その新たな通信端末の送受信する通信情報は暗号化により漏洩から保護され、その新たな通信端末のネットワーク資源の利用に関しては不正な利用が防止される。

【図面の簡単な説明】

【図1】 本発明の第1実施形態における無線通信システムの概要構成を示す図である。

【図2】 本発明の第1実施形態における携帯型情報端末の概要構成を示す図である。

【図3】 本発明の第1実施形態における携帯型情報端末のプロトコル情報ファイルの構成を示す図である。

【図4】 本発明の第1実施形態における携帯型情報端末の暗号鍵情報ファイルの構成を示す図である。

【図5】 本発明の第1実施形態における携帯型情報端末の端末情報ファイルの構成を示す図である。

【図6】 本発明の第1実施形態における無線通信に関する設定の動作例を示すフロー図である。

【図7】 本発明の第2実施形態における無線通信システムの概要構成を示す図である。

【図8】 本発明の第2実施形態における通信端末の概要構成を示す図である。

【図9】 本発明の第2実施形態における通信端末の設定管理情報ファイルの構成を示す図である。

【図10】 本発明の第2実施形態における通信端末、および第3実施形態における有線通信部を有する通信端末の端末情報ファイルの構成を示す図である。

【図11】 本発明の第2実施形態における通信端末、第4実施形態における新規参入する通信端末、および第4実施形態におけるアクセスポイントの自機プロトコル情報ファイルの構成を示す図である。

【図12】 本発明の第2実施形態における通信端末、第3実施形態における有線通信部を有する通信端末、第4実施形態における新規参入する通信端末、および第4実施形態におけるアクセスポイントの他機プロトコル情報ファイルの構成を示す図である。

【図13】 本発明の第2実施形態における通信端末、および第4実施形態における新規参入する通信端末およびアクセスポイントの決定プロトコル情報ファイルの構成を示す図である。

【図14】 本発明の第2実施形態における無線通信に関する設定の接続認証段階の動作例を示すフロー図である。

【図15】 本発明の第2実施形態における無線通信に関する設定のマスタ・スレーブ決定段階の動作例を示すフロー図である。

【図16】 本発明の第2実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。

【図17】 本発明の第2実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。

【図18】 本発明の第3実施形態における無線通信システムの概要構成を示す図である。

【図19】 本発明の第3実施形態における有線通信部を有する通信端末の概要構成を示す図である。

【図20】 本発明の第3実施形態における有線通信部を有する通信端末の設定管理情報ファイルの構成を示す図である。

【図21】 本発明の第3実施形態における有線通信部を有する通信端末の自機プロトコル情報ファイルの構成を示す図である。

【図22】 本発明の第3実施形態における有線通信部を有する通信端末の決定プロトコル情報ファイルの構成を示す図である。

【図23】 本発明の第3実施形態における有線通信部を有する通信端末および有線通信部を有さない通信端末、第4実施形態におけるアクセスポイントの識別子情報ファイルの構成を示す図である。

【図24】 本発明の第3実施形態における有線通信部を有する通信端末および有線通信部を有さない通信端末の公開鍵情報ファイルの構成を示す図である。

【図25】 本発明の第3実施形態における有線通信部を有さない通信端末の概要構成を示す図である。

【図26】 本発明の第3実施形態における有線通信部を有さない通信端末の設定管理情報ファイルの構成を示す図である。

【図27】 本発明の第3実施形態における無線通信に関する設定の接続認証段階の動作例を示すフロー図である。

【図28】 本発明の第3実施形態における無線通信に関する設定のパラメータ設定段階の動作例を示すフロー図である。

【図29】 本発明の第3実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。

【図30】 本発明の第3実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。

【図31】 本発明の第4実施形態における無線通信システムの概要構成を示す図である。

【図32】 本発明の第4実施形態における新規参入する通信端末の概要構成を示す図である。

【図33】 本発明の第4実施形態における新規参入する通信端末の設定管理情報ファイルの構成を示す図である。

【図34】 本発明の第4実施形態におけるアクセスポイントの概要構成を示す図である。

【図35】 本発明の第4実施形態におけるアクセスポ

イントの設定管理情報ファイルの構成を示す図である。
【図36】 本発明の第4実施形態におけるアクセスポイントのアクセス権限情報ファイルの構成を示す図である。

【図37】 本発明の第4実施形態におけるアクセスポイントの共通鍵情報ファイルの構成を示す図である。

【図38】 本発明の第4実施形態における新規参入する通信端末以外の通信端末の概要構成を示す図である。

【図39】 本発明の第4実施形態における新規参入する通信端末以外の設定管理情報ファイルの構成を示す図である。

【図40】 本発明の第4実施形態における無線通信に関する設定の接続認証およびパラメータ設定段階の動作例を示すフロー図である。

【図41】 本発明の第4実施形態における無線通信に関する設定の接続認証およびパラメータ設定段階の動作例を示すフロー図である。

【図42】 本発明の第4実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図であ

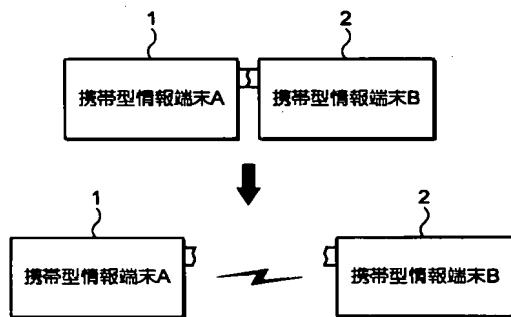
る。

【図43】 本発明の第4実施形態における無線通信に関する設定完了後の通信の動作例を示すフロー図である。

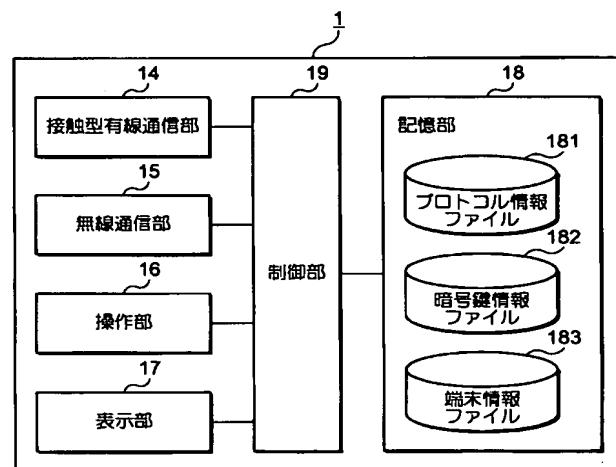
【符号の説明】

- 1, 2 携帯型通信端末
- 3, 4, 5, 6, 7, 8, 9, 11, 12 通信端末
- 10 アクセスポイント
- 13 ネットワークサーバ
- 14 接触型有線通信部
- 15, 21, 28, 34, 41, 48 無線通信部
- 16, 22, 29, 35, 42, 54 操作部
- 17, 23, 30, 36, 43, 55 表示部
- 18, 25, 32, 38, 45, 51, 57 記憶部
- 19, 24, 31, 37, 44, 50, 56 制御部
- 20, 27, 49 有線通信部
- 26, 33, 39, 46, 52, 58 バス
- 40, 47 赤外線通信部
- 53 通信部

【図1】



【図2】



【図3】

プロトコル	MACアドレス	パラメータセット		優先順位
		パラメータ1	...	
IEEE802.11b	00601D038703	チャネルID=1	...	1
Bluetooth	6ABE1D01C87A	PIN Code=1234	...	1
...
...

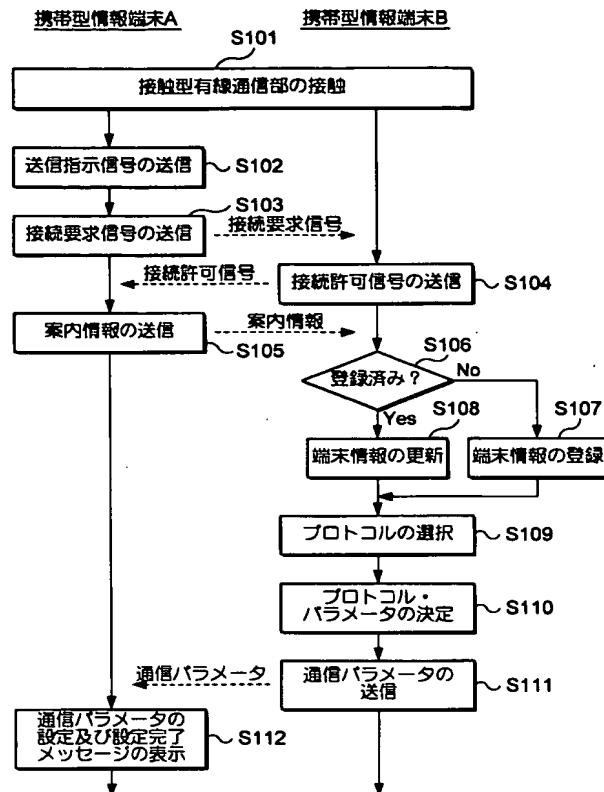
【図4】

識別子	暗号鍵
EP00002	3d068c4a50

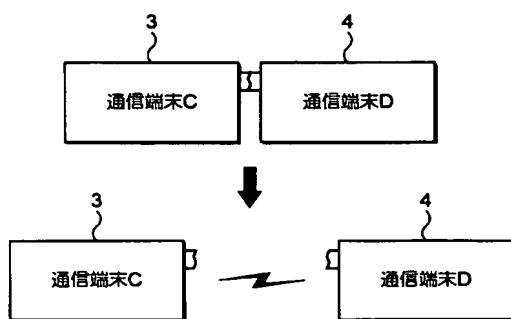
【図5】

183				
識別子	アクセス権限	暗号鍵	プロトコル	MACアドレス
EP00001	読み取り専用	07003e8b4a	Bluetooth	00601D038702
EP00003	フルアクセス	top5ofb2wg	IEEE802.11b	00601D038705
⋮	⋮	⋮	⋮	⋮

【図6】



【図7】



【図9】

251	
マスタ・スレーブ	1
自機識別子	0585CA2C
他機識別子	BC5E7DC0
パスワード	AZ23#c7
共通鍵	v1h4e5jqxhp3em6feak#vcun
設定完了通知フラグ	OFF

【図10】

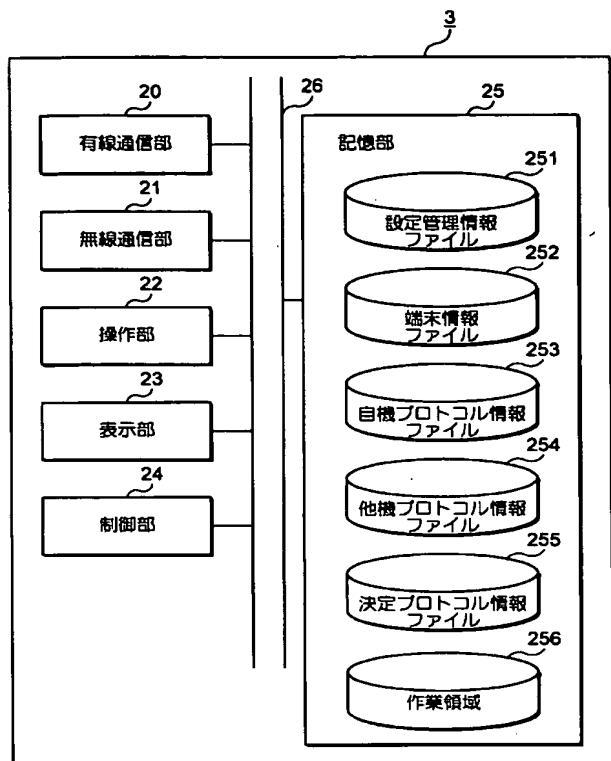
252	
識別子	
57242C0D	
BBA60A16	
⋮	

254	
MACアドレス	プロトコルセット
58DF46499F0C	IEEE802.11b - TCP/IP
58DF46499F0C	IEEE802.11b - IPX/SPX
C59166816E84	HomeRF - NetBEUI
⋮	⋮

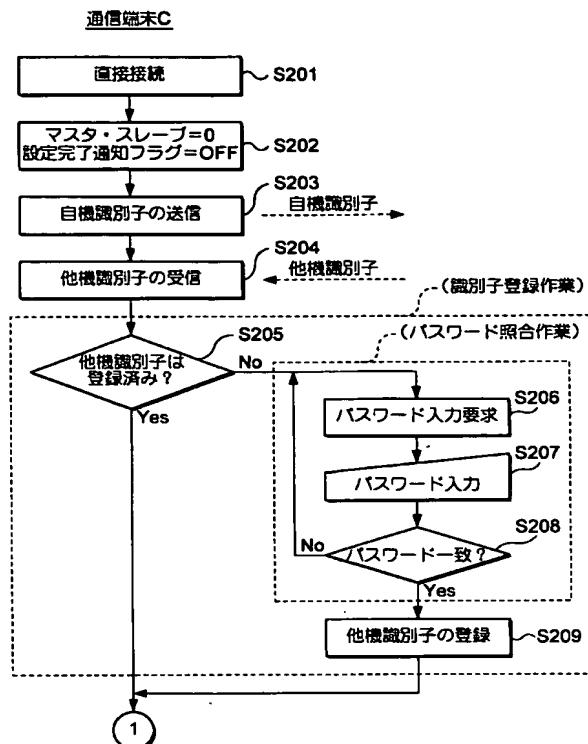
【図13】

自機MACアドレス	他機MACアドレス	プロトコルセット	パラメータセット			
			パラメータ1	パラメータ2	パラメータ3	⋮
5B98007E03E2	58DF46499F0C	IEEE802.11b - TCP/IP	IEEE802.11b - AdHoc	IEEE802.11b チャンネルID=5	IPアドレス/サブネットマスク 192.168.0.221/255.255.255.0	⋮

【図8】



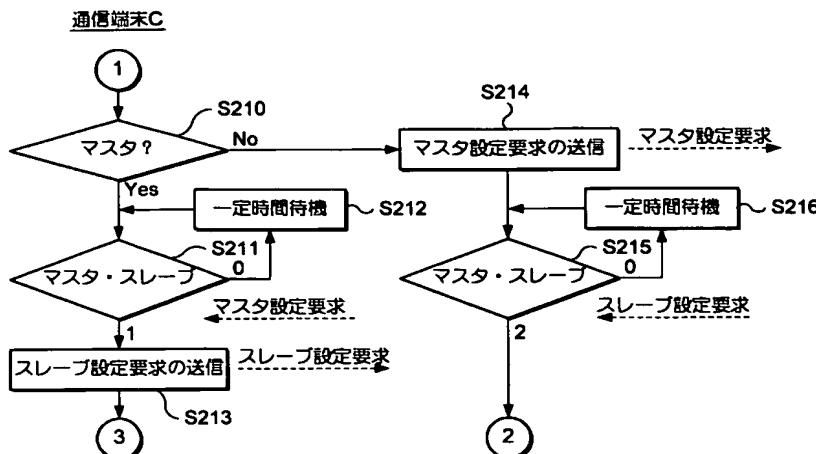
【図14】



【図11】

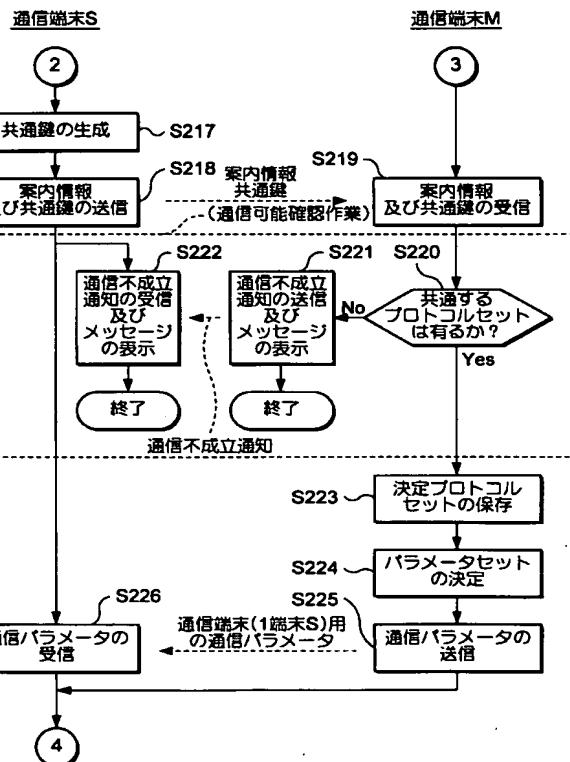
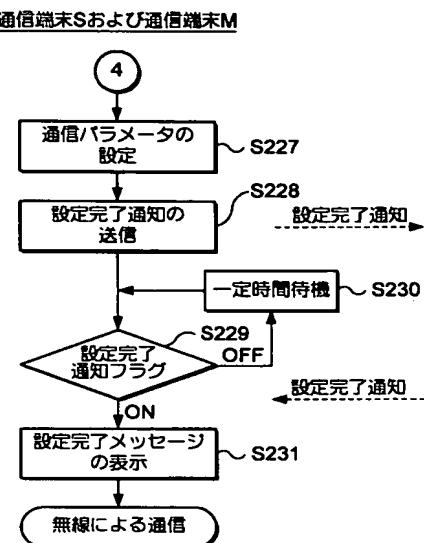
優先順位	MACアドレス	プロトコルセット	パラメータセット			
			パラメータ1	パラメータ2	パラメータ3	...
1	E8B0324FC8E5	IEEE802.11b - NetBEUI	IEEE802.11b モード=AdHoc	IEEE802.11b チャネルID=7	—	...
2	5B98007E03E2	IEEE802.11b - TCP/IP	IEEE802.11b モード=Infrastructure	IEEE802.11b チャネルID=3	IPアドレス/サブネットマスク 192.168.0.220/ 255.255.255.0	...
3	F0A6998BF3CB	Bluetooth - NetBEUI	Bluetooth PIN Code=2851	—	—	...
...

【図15】

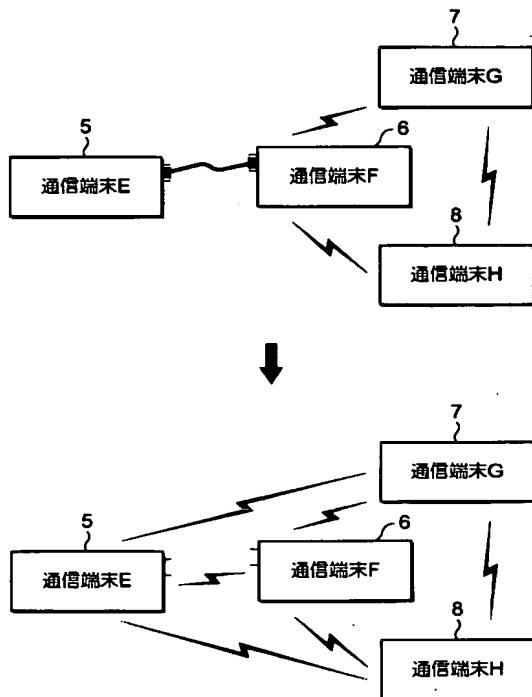


【図16】

【図17】



【図18】



【図26】

【図35】

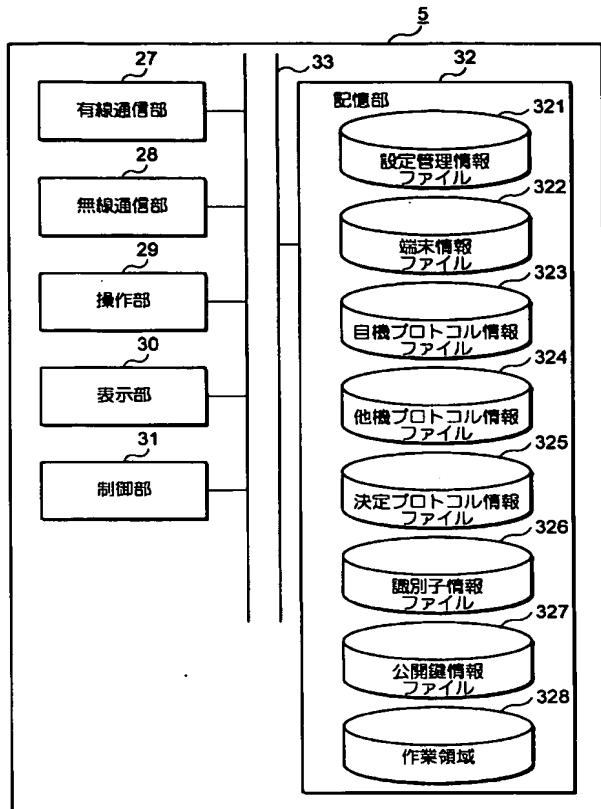
381

自機識別子	3869B1F4
秘密鍵	zw1y3u3g&uk5onlnls1mnIk\$
公開鍵	oc#&m6lbs%z7v#hip3ztha&1

511

他機識別子	D24F7B85
他機公開鍵	10tiz9#0vj5mcicqgqb1j3z9b

【図19】



【図20】

自機識別子	19ABB17A
パスワード	7bAlk8b#
秘密鍵	law#q&s26f9ry3q%soo%tieu
公開鍵	gc3rxwzjrf946s29p25c\$mp

【図23】

MACアドレス	識別子
B7614A795845	34FA9FF7
5FFD147EFFFF	32CCA022
ABF82A04D002	32CCA022
48D6A6626071	942D7BE6
⋮	⋮
⋮	⋮

【図21】

MACアドレス	プロトコルセット	パラメータセット			
		パラメータ1	パラメータ2	パラメータ3	⋮
A05CBE6ADEE5	IEEE802.11b - NetBEUI	IEEE802.11b モード = AdHoc	IEEE802.11b チャネルID = 5	—	⋮
A05CBE6ADEE5	IEEE802.11b - TCP/IP	IEEE802.11b モード = AdHoc	IEEE802.11b チャネルID = 5	IPアドレス/サブネットマスク 192.168.0.60/ 255.255.255.0	⋮
BB2214AA3C1A	Bluetooth - NetBEUI	Bluetooth PIN Code = 7218	—	—	⋮
⋮	⋮	⋮	⋮	⋮	⋮

【図22】

325

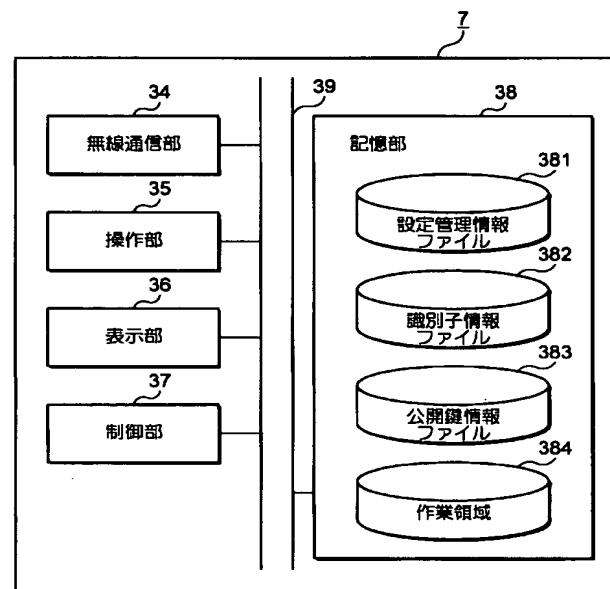
自機MAC アドレス	他機MAC アドレス	プロトコル セット	パラメータセット			
			パラメータ1	パラメータ2	パラメータ3	...
A05CBE6ADEE5	5FFD147EFFFF	IEEE802.11b - TCP/IP	IEEE802.11b モード=AdHoc	IEEE802.11b チャンネルID=3	IPアドレス/マスク 192.168.0.222/ 255.255.255.0	...
BB2214AA3C1A	ABF82A04D002	Bluetooth - NetBEUI	Bluetooth PIN=4E63	—	—	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図24】

327

識別子	公開鍵
0243B88E	tjfsjwrz#e5eyega\$27db#%8
32CCA022	u#y#09v\$3jqa%ivvz5ya0m5
3869B1F4	oc#&m6lbs#z7v#hipztha&1
⋮	⋮
⋮	⋮
⋮	⋮

【図25】



【図33】

451

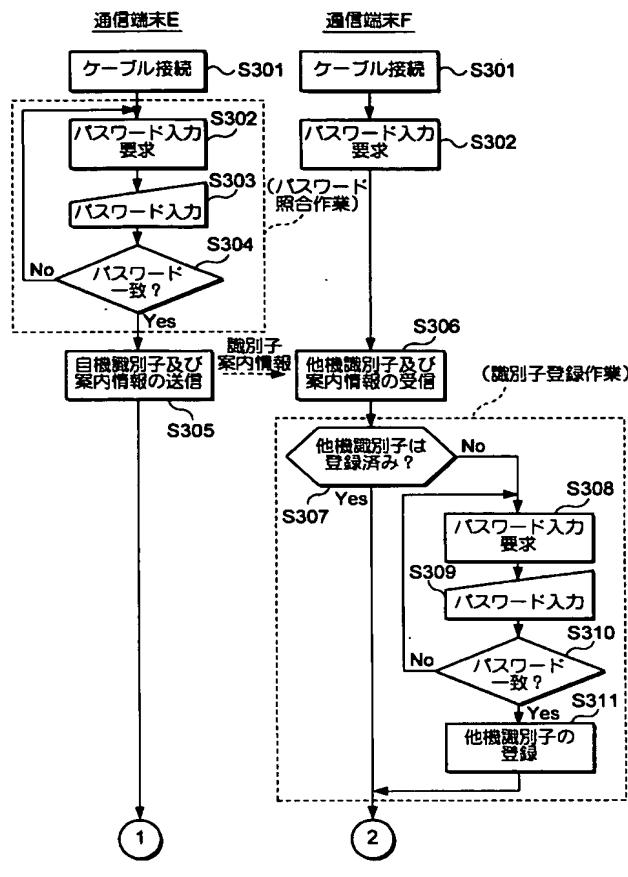
自機識別子	D24F7B85
パスワード	&rTqk\$Q1
秘密鍵	\$8#fsbnff#y0tm8o3qml\$36s
公開鍵	10tiz9#0vj5mcijggqb1j3z9b
共通鍵	#08dvq763&qkyda52xhua022

【図36】

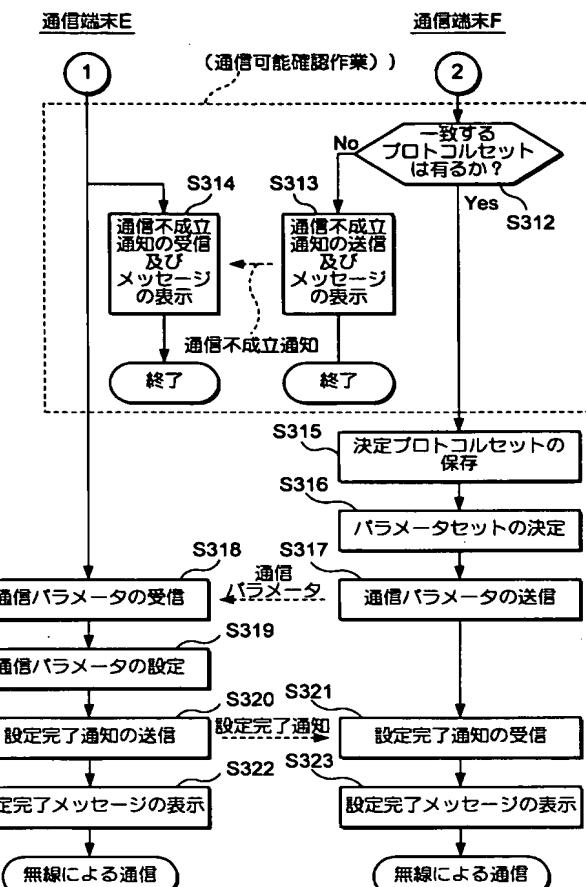
512

識別子	アカウント・グループ
8B78BF6A	同支部同セクション
D24F7B85	他支部
0C485394	同支部他セクション
⋮	⋮
⋮	⋮
⋮	⋮

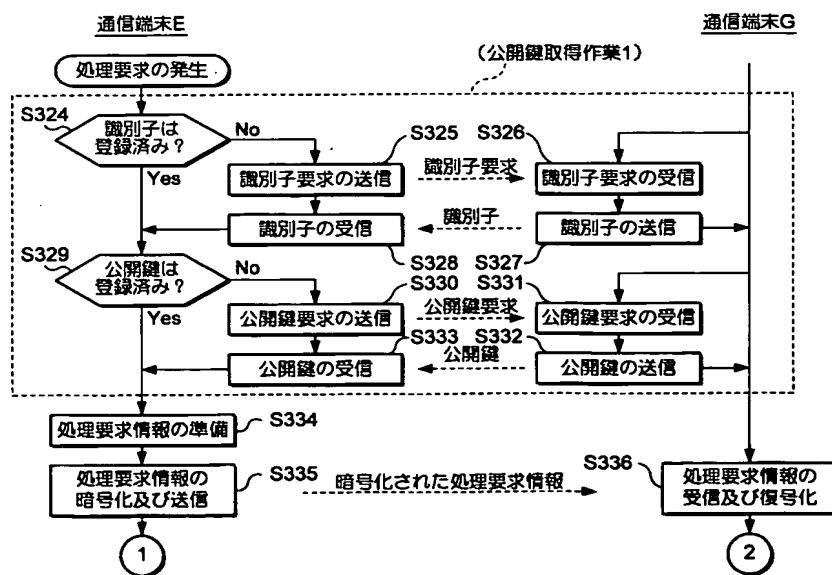
【図27】



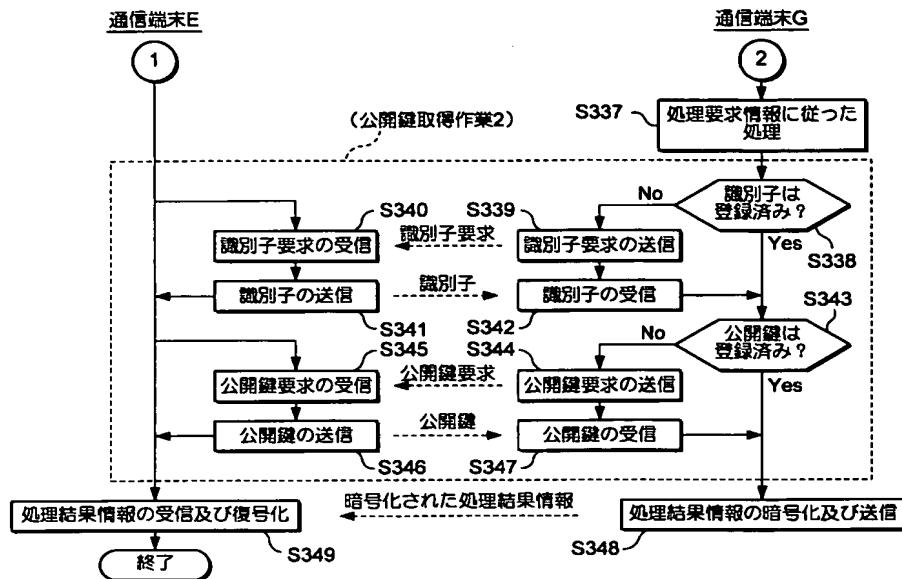
【図28】



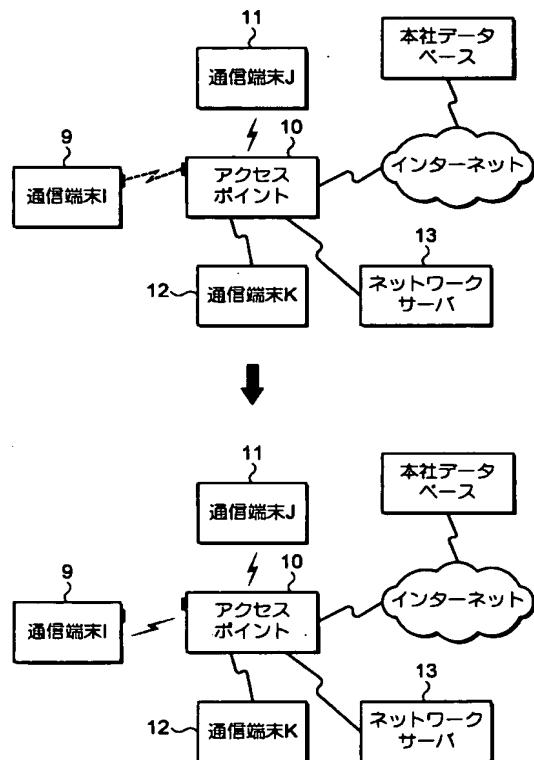
【図29】



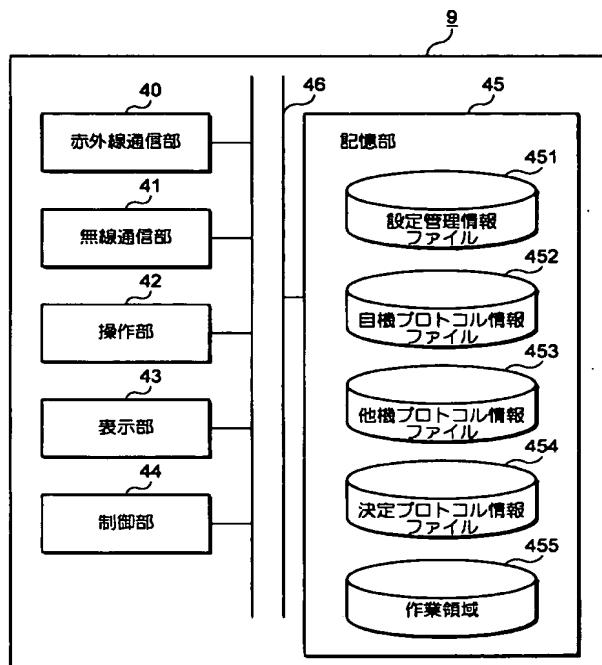
【図30】



【図31】



【図32】

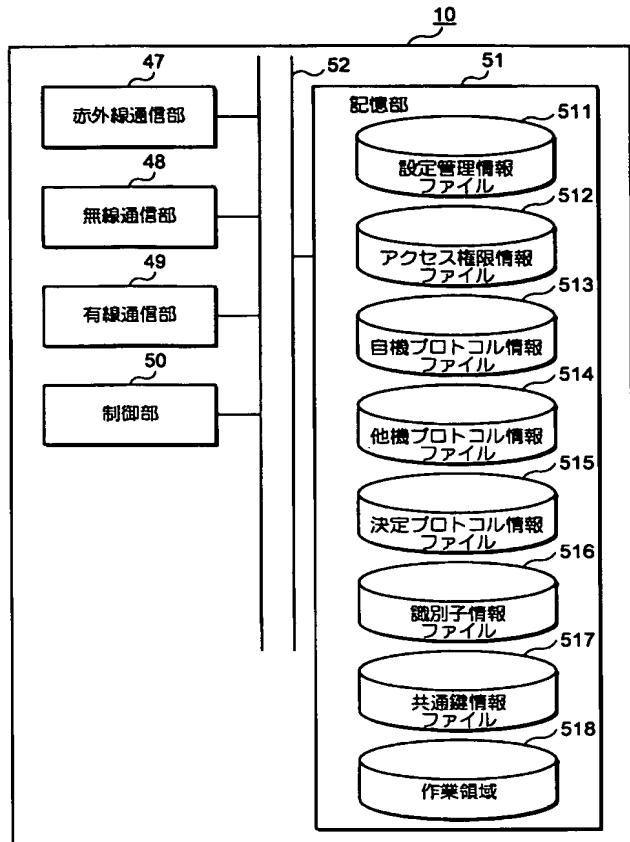


【図39】

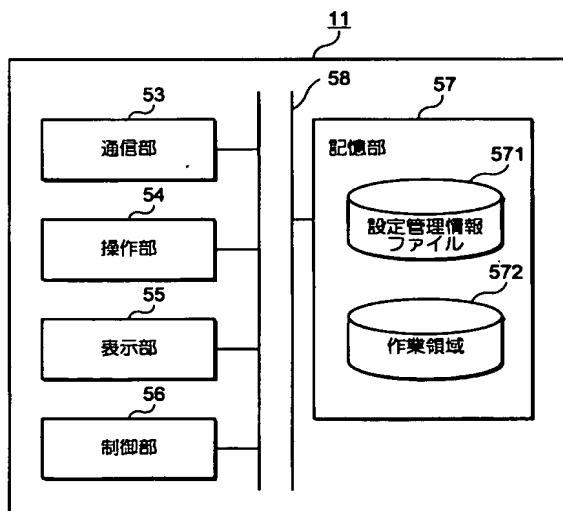
571

自機識別子	46EB8684
共通鍵	2%76o7kimv8l3cw9#ume5qo6

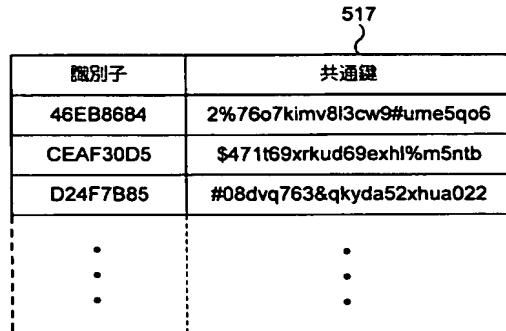
【図34】



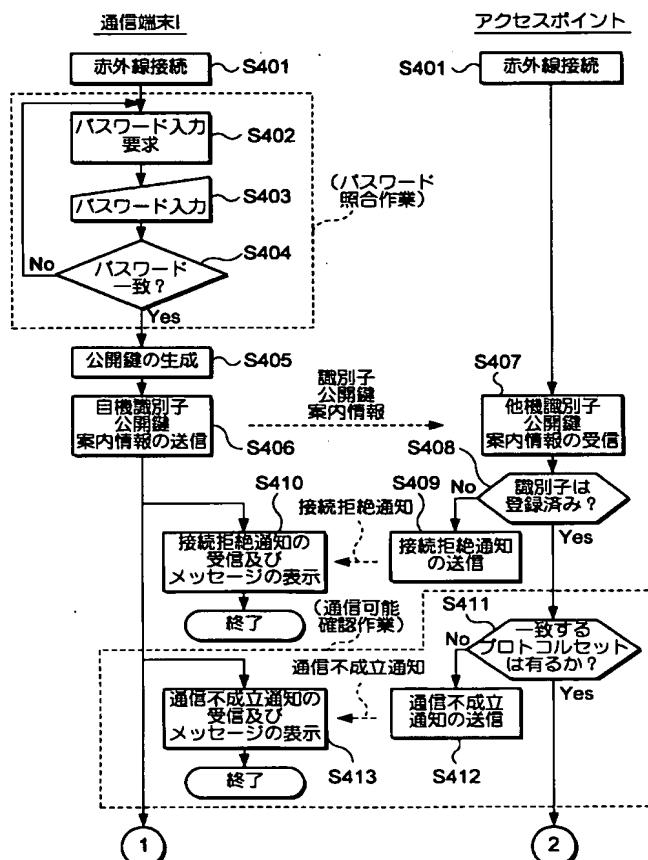
【図38】



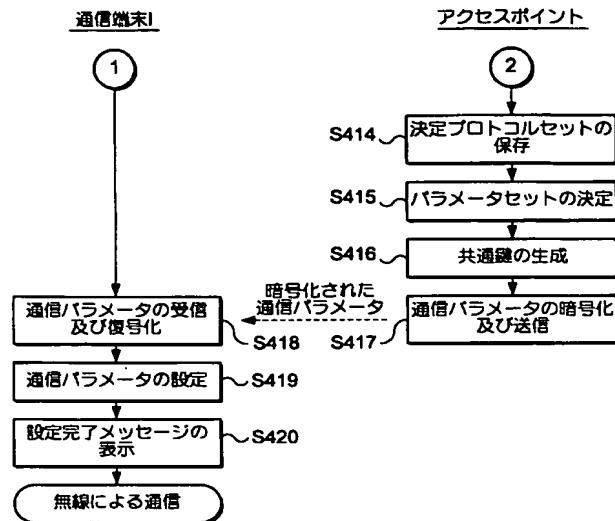
【図37】



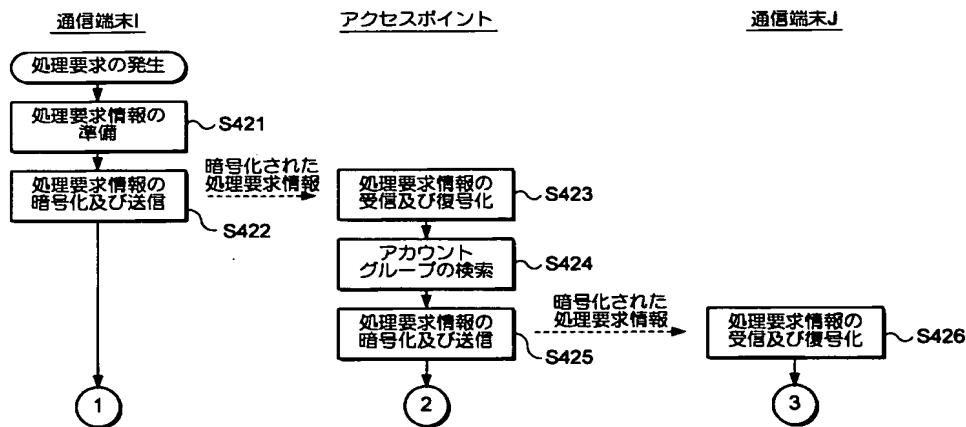
【図40】



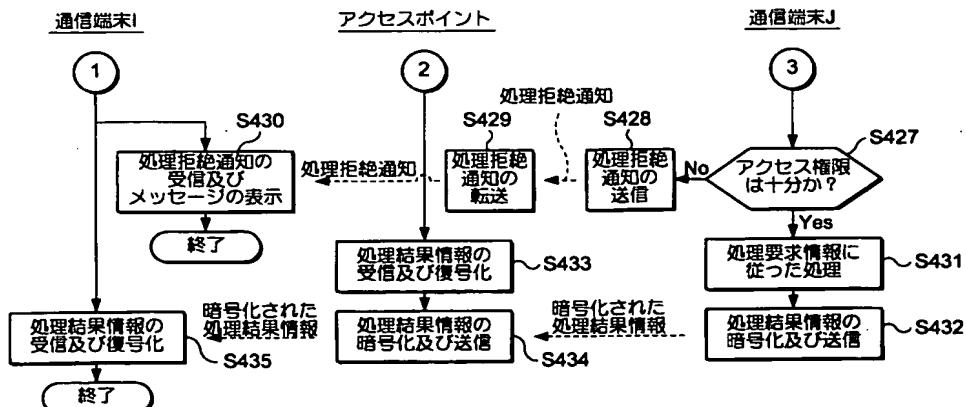
【図4-1】



【図4-2】



【図4-3】



フロントページの続き

(51) Int.C1. ⁷	識別記号	F I	マークコード(参考)
H 0 4 Q	7/26		
	7/30		
	7/38		
(72)発明者 山門 均		F ターム(参考)	5K033 DA19 DB12 DB14 ECO1
長野県諏訪市大和3丁目3番5号	セイコ		5K034 AA19 EE03 EE11 HH63 MM39
一エプソン株式会社内			5K067 AA21 BB02 BB21 DD11 DD51
(72)発明者 宮本 徹			EE02 EE10 EE16 HH11 HH22
長野県諏訪市大和3丁目3番5号	セイコ		HH36
一エプソン株式会社内			